T-Codes, Tables, Reports & Authorization Objects.

T-Codes (Transaction Codes)

SICK – To check weather SAP is installed properly or not.

SM50 – To check the status of particular instance of work process.

SM66 – To check the status of all the instances of work process.

SM51 – To check the status of the server ~~weath~~ wheather server is active/inactive

SE16/SE16N – To check the table.

SA38 – To generate Reports.

SM04 – List of all active users for a particular instance.

AL08 – List of all active users for all instances.

User Administration T-codes:-

SU01 – Single User Maintainence.

SU10 – Mass/Multiple user Maintainence.

SU01D – Can display all the users and data (same as display(60)-tab in su01).

SU1M – log info (monitors and has every data recorded which we have done).

User Groups:-

SUGR – Helps to create User group.

SCC4 – Helps to create client by BASIS consultants & also client administration. (critical T-code).

SCC5 – T-code helps to delete a client (critical client) (in production)

~~T000~~ – ~~List of all clients in the system.~~

SM01 – Helps to lock / unlock T-codes in the system.

~~TCTC~~ – ~~To check all the T-codes in the system.~~

SM01-DEV → Helps to lock T-code in the development system and it can be transfered to Production.

SM01-CUST → To lock T-code for a time being.

SU21 – Helps to generate sap-all.

SM30 – Modifying any table (we modify only USR40).

EW25 – Helps to lock 'all' users.

RZ10 – Helps to change the parameter values.

RZ11 – Helps to check the information of parameters.

Secpol – Helps to maintain specific password policy to some main users.

SE13 – 2nd prerequisite helps to maintain Technical settings (Tables) in SAP. (modification of tables related T-code).

SCU3 – Helps to retrive data. (modifications of tables related T-code).

SE06 – Helps to modify system Globally.

ME21N – Helps to create purchase order in SAP.

Rec/client – 1st prerequisite and static parameter helps to find data who has modified in the table.

ME22N – Helps to change the purchase order.

ME23N – Helps to display the purchse order.

Sales Department:-

VA01 – This t-code helps to create Sales Order.

VA02 – This t-code helps to change sales order.

VA03 – This t-code helps to display sales order.

SE37 – This t-code helps to lock/unlock clients.

CUA - Central User Administration:-

BD54/SALE – Helps to create logical systems. (client eg:- 810).

SCC4/SALE – We assign logical system to appropriate client.

SM59 – To create RFC.

SCUA – We need to attach/assign all the child systems to parent systems.

~~TALT~~ – ~~All activities are~~

SCUM – Where you maintain field parameters (tabs in SU01) } These execute only when CUA communication is available

SCUG – To transfer child system users to parent systems.

SCUL – Gene Helps to Generate locks (CUA).

Procurement Cycle:-

ME51N – Helps to purchase Requisition.
ME52N – Helps to change purchase Requisition.
ME53N – Helps to Display Purchase Requisition.
ME41 – Helps to create RFQ (Request for Quotation)
ME42 – Helps to change RFQ.
ME43 – Helps to display RFQ.
ME28 – Helps to Approve PO (Purchase Order).
ME45 – Helps to Release RFQ.
MIGO – Helps for Goods Movement in SAP.
PFCG – Helps to create Role.
XK01 – Helps to create Vendors.

End user T-codes:-

SU0 - User can modify default values.
SU1 → User can modify address info.
SU2 → user can modify parameters info.
SU3 → Users can modify address, defaults, Parameters info (combination of SU0+SU1+SU2).

User Buffer:-

SU56 → Authorization objects, Roles, profiles, values stores in this and to reset user buffer.

Table Security:-

SE54 → To create customized user ~~table~~ groups and assign to the user.

SE38 → To create Program.

SU21 → for (Security Consultant) you can identify that how many fields are there and what are the permitted activities are there in the particular Authorization Object. for (ABAPERS) want to create customized object classes & also creating of authorization object.

SE93 → To create our own customized T-codes.

SU20 → To maintain Authorization fields (for ABAPERS).

SUPC → To generate Mass Profiles.

SU53 → To evaluate last failed authorization check (what is missing to user).

ST01 → To enable the Trace.

Stauthtrace → (Where we can skip two (steps ALOS & SMX1) same as ST01 to enable trace for any instance/client/system using their User Id's.

SU22 → When we install SAP default values are stored in this tables (user Auth. Objs are pulled from some others).

SU24 → same as SU22 but USOBT-C contains no values.

SU25 → This Tcode helps to Transport data from ~~USOB~~ SU22 to SU24 (This is one time activity).

SE01 → To transport Request.

SE09, SE10 → T-codes helps to transport Request/change text also (short description)

E070 :→ Table F-code shows the status of Transport Request (i.e Released/Modified).

E071 :- Table Actual Data (objects with in Transport Request) eg: Roles, Programs.

PFUD :- Which will help you to do mass comparision to user.

SM36 :- Helps to schedule a background job

SM37 :- To monitor a background job

SMX :- This helps to check the Background job for the user by himself/Directly shows the status.

SECATT :- This Tcode helps to perform test script and test configuration and also uploading file job.

SE03 :- Helps to change comment (which we have have previously given in Transport)

SQVI :- Helps to Merge tables.

PFCGMASSVAL :- Directly we can maintain values for all authorization fields.

FK01, XK01 :- Helps to create vendors.
↓ finance point of view ↓ from purchase point of view.

RSPFPAR - LOGIN →

STMS - Transport Request Status (in which status. in QAS, or PRD, DEV).

SCC1 - To request Transport from one client ~~(QAS)~~ to other client.

Tables

USR01 – Holds all the user master data. (Defaults tab info)

USR02 – User logon Master information (data of passwords & users, Logon tab data)

USGRP – Displays the user groups. (Groups tab)

USGRP_USER – Relation ship between usergroup & user (Groups tab).

USGRPT – To view the text given to user group.

USREFUS – Relationship between dialog and reference user.

T000 – List of all clients in the system. (critical table)

USR40 – Maintains data of Illegal Passwords.

USR03 – User Address Information (Address tab)

T001 – Holds the data of company codes of finance department (critical)

T001W – Holds the data of company's plants / Branches (critical table).

T001L – Holds the data of storage locations of companies (critical table).

MARA – Holds the information of material of the company (critical table)

MARD – Holds the information of storage location of material. (critical Table).

TSTC – Holds the list of all T-codes in the system.

DBTABPRT – Helps to retrive data log records, changes are stored in this table. (Max we use SCU3 t-code).

DBTABLOG – Helps to retrive data log records are stored in this table.

CUA – Central User Administration;-

TBDLS – List of logical systems can be seen in this table.

TACT – All activities are stored (01, 02, 03, 04, 05, 06, 16, 22) (01 create, 02 change, 03 display, 04 print, 05 lock/unlock, 06 delete, 16 execute, 22 enter, include assign)

TOBC – This tables should stores list of all object class

TOBJ – This table stores list of all authorization object.

USR05 – Relation ship between Parameter and user can be seen in this table.

USVAR – Technical names for Org levels can be found.

AGR-AGRS – Relation ship between single role & composite role.

AGR_USERS – List of users assigned to the roles

AGR_NUM_2 → Helps to show list of Profile names.

AGR_Tcode → This show Relationship between Role & T-code.

USR04 → Relation ship between User and profile.

AGR_Define → Relation between Master role & derived role.

AGR_1251 → List of fields and values in a role

AGR_1252 → List of org levels and values of a role.

TDDAT → To check in which group the table belongs to. (Table security).

TDDAT → To check how many tables are there in that particular group.

TACTZ → To identify that how many fields are there and what are the permitted activities are there in particular Authorization Object. (If we don't have access for SU01 we use this).

Devaccess → Stores the Access key of ABAP users (20 characters) and to know how many developers are there in the system.

Adiraccess → All the object keys are stored (accessed).

TSTCP → Substitute T-codes are stored in this table.

TPARA → List of parameters

USR07 → List of last failed authorization check.

TSTCT → Text of all T-codes.

USBO USOBX → contains object class, Authorization object, fields (in SU22)

~~USOBX~~ USOBT → contains values (default given values) (in SU22)

USOBX_C (copy/change) → object class, Authorization objects, fields. (in SU24)

USOBT_C → this table is empty (when pulled from SU22 contains values). (SU24).

TBTCP → This table shows for particular program name what background job is scheduled will

TBTCO → This table shows when the Background job is scheduled, time and status of (Background jobs).

E070CREATE → Shows created Requests of Transport requests (no values found when the Request is released).

Agr_1016 → Shows how many profiles are created for a role

Agr_Prof → shows current profile available with a role.

USR41 → In which instance user is logged in (don't have access of AL08 & SM04)

SA38:

Reports

RSUSR003 - Checks weed whether standard user's Password changed or not.

RSAUDITC - To check the locked T-codes.

RSUSR406 - If SU21 access has not given we use this report to generate sap_all. (critical).

RSUSR200 - To check user types (also finds other user information)

RSUSR006 - List of users last logon data and password change also displays user lock status.

RSUSR003 - Displays users with incomplete address data.

RSPFPAR - Helps to search a particular parameter.

RSPARAM - Helps to search all parameters.

RSDELCUA - To delete CUA (central User Administration) configuration.

RSUSR405 - To reset user Buffer for all the users.

PFCG_MASS_TRANSPORT → When there is no access for PFCG to transport Roles we use this Report to transport.

PFCG-time_Dependant → When there is no access to PFUD to user we use this report. It does user profile comparision to user.

PRGN_COMPRESS_TIMES → Report to delete expired role entries and also duplicate roles can will be deleted.

Mitigation - Detective control

Remediation - Protective Control.

S – Tcode (common for all) **Authorization Objects**

Related to SU01

S – user – grp
S – user – pro
S – user – SAS
S – user – ~~grp~~
S – user – sys
S – user – Aut
S – Secpol.

Table Security

S – tabu – dis
S – tabu – nang
S – tabu – cli
S – tabu – lin
S – User – val
S – user – TCD
S – user – ADM

RFC

S – RFC
S – RFC – ADM

Background Job

S – Btch – Job
S – Btch – Nam
S – Btch – Adm

Developers

S – Develop
S – program.

Related to MM01 (material management (functional))

M – MATE – MAN
M – MATE – MAR
M – MATE – MAT
M – MATE – MEX
M – MATE – VKO
M – MATE – WGR
M – MATE – WRK.

Vendor Master

F – LFA1 – BEK
F – LFA1 – BUK
F – LFA1 – GRP
F – LFA1 – AEN

Customer Master

F – KNA1 – BED
F – KNA1 – BUK
F – KNA1 – KGD
F – KNA1 – AEN

Goods

M – MSEG – BWE
M – MSEG – WWE

Banking Master Records

F – BNKA – BUK
F – BNKA – MAN

payment Card data

B – CARD – SEC
B – CCARD.

Transport

S – Transport
S – cts – adm

Parameters RZ10 & RZ11

S – RZL – ADM
S – GUI (Actvt = 60 (export), 61 (Import).

Upload & download Tables

S – GUI
(Actvt – 60 (export), 61 (Import).

Shravya

Running Notes

Table of Contents:

Introduction (1 - 10)

User Administration (11 - 13)

U-flag Values (14)

User Groups (14 - 15)

Powerful profiles (17)

User Types (20 - 24)

Lock/unlock Tcode (24)

Illegal Passwords (26 - 30)

Data Types (29), Systemprofiles.

Secpol (35)

Rec/client (36 - 37)

CUA (41 - 45)

User Defined Parameters (48 - 49)

Roles (49 - 56)

Table Security (59 - 62)

SU53 (last faild Authcheck) (64 - 65)

Trace (65 - 67)

SU22, SU24, SU25 (68 - 70)

Transporting (70 - 73)

Background job (73 - 75)

Ecatt (79 - 82)

Merging Tables (82 - 83)

Sap-all display mode (83 - 84)

Market place (86)

How profile is generated (53 - 54)

Security Hirarchy (47)

What happens when we add T.code (53).

RZ10, RZ11 - pfcg (29)

Activities (45)

Tabs related tables in SU01 - (30)

INTRODUCTION TO SAP

SAP - Systems, Applications & products in Data processing.

ERP - Enterprise Resource planning.

→ ERP is a software which is distributed according to the company needs

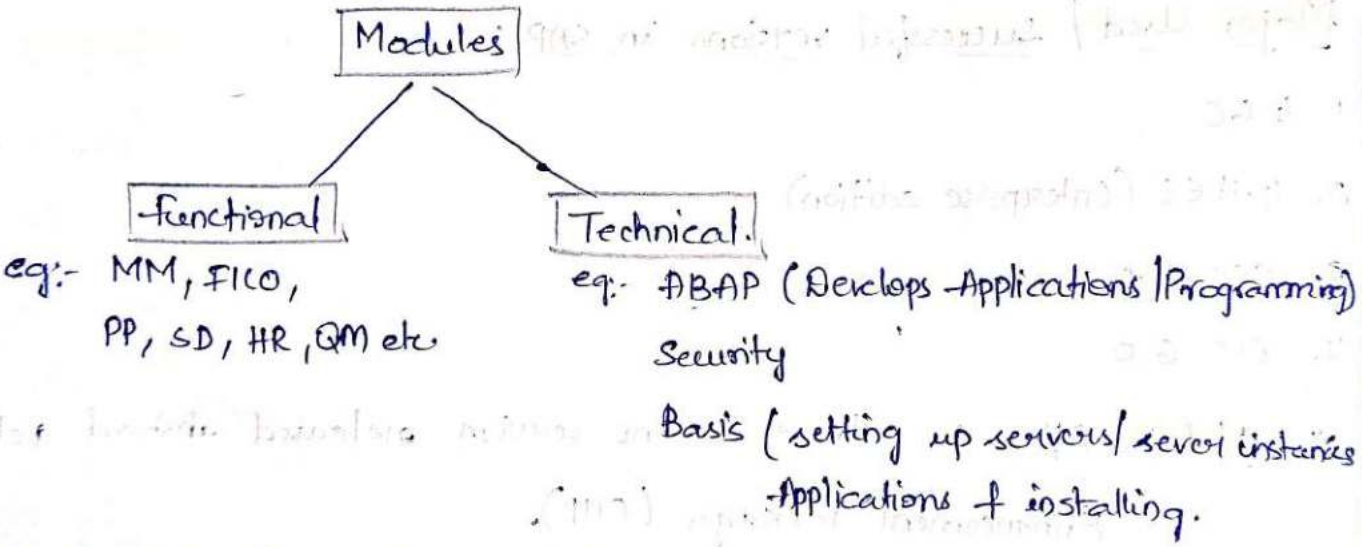
→ SAP is a multinational company which provides ERP as per the company requirements.

→ There are several kinds of departments like financial, sales, production, Material Management etc.

→ The word department is called as Module in SAP terminology.

ABAP → Advanced Business Application Programming.

BASIS → Business Application Software Integrated solution.


Modules
Functional
eg:- MM, FICO, PP, SD, HR, QM etc
Technical.
eg:- ABAP (Develops Applications / Programming)
Security
Basis (setting up servers / several instances Applications & installing.

Security:- It helps to create userid's, gives roles, and can give restrictions as per the requirement (roles). (knowing the commands and execute them)

Project types in SAP:-

1. **Implementation** :- It helps to develop a project from scratch.
2. **Support** :- Giving support to project by rectifying errors & bugs.
3. **Upgrade** :- Upgrading to one version to other version.
4. **Roll out** :- Expanding the business from one location to others.
5. **Migration**:- Implementing ~~from~~ Migrating from one s/w / H/w to other different s/w / H/w.

Versions in SAP:-

* 1st version → SAP R1 in 1972.
  2nd version → SAP R2 in 1978.
  3rd version → SAP R3 in 1992.

'R' indicates Real time 3 tier 1 architechture
" 2 "
"

⋮	1.0
⋮	1.1
⋮	⋮
SAP R3	4.6A
SAP R3	4.6B
SAP R3	4.6C
Ecc	5.0
Ecc	6.0

ECC - Enterprise Core Component.

Major Used / Successful versions in SAP :-

1. 4.6C
2. 4.7 EE (Enterprise edition)
3. ECC 5.0
4. ECC 6.0

* Note :- After 6.0 there are no versions released instead releases Enhancement Packages (EHP).

* Which version you are working on?

A:- Ecc 6.0

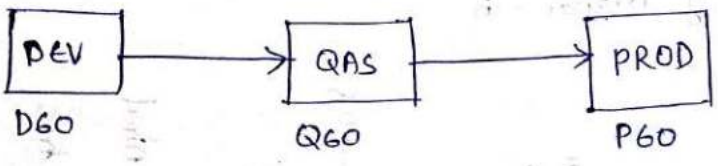
Q With which EHP you are using?

A:- 6. ~~(EHP 6)~~. (EHP 6).

→ Enhancement package (1, 2, 3, 4 ---- 8)
(new & improved s/w). (n-1)

* We only use (n-1) EHP until the next upgradation EHP 9.

SAP Landscape :- Arrangement of servers



→ need to install SAP in above all three servers.

→ It is unidirectional.

→ If a program is done it is sent to QAS and will be checked by the change owners if there are, any changes required then the new object is created in DEV server ~~but soon~~ if no changes it is sent to PROD.

→ We identify a person/employee who is working on which server can be identified by using (SID): system Identifier.

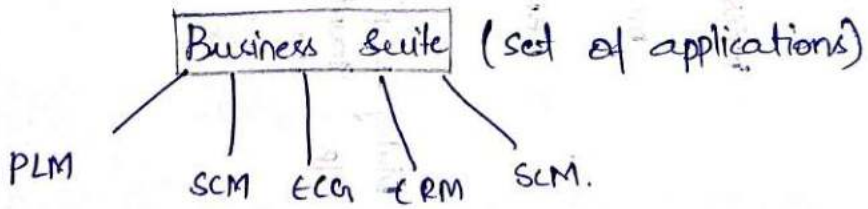
System Identifier:-

* It contains 3 letters
* Out of 3 1st letter should be Alphabet remaining 2 should be alphanumeric

Eg:- 1) S0D 2) MD1 (∵ It will be easy if there will be ~~one~~ D, P, Q in each SID's).
S1Q MQ2
S2P MP3

→ BASIS consultants creates SID's.

→ like MS office in windows we use Business suite in SAP.



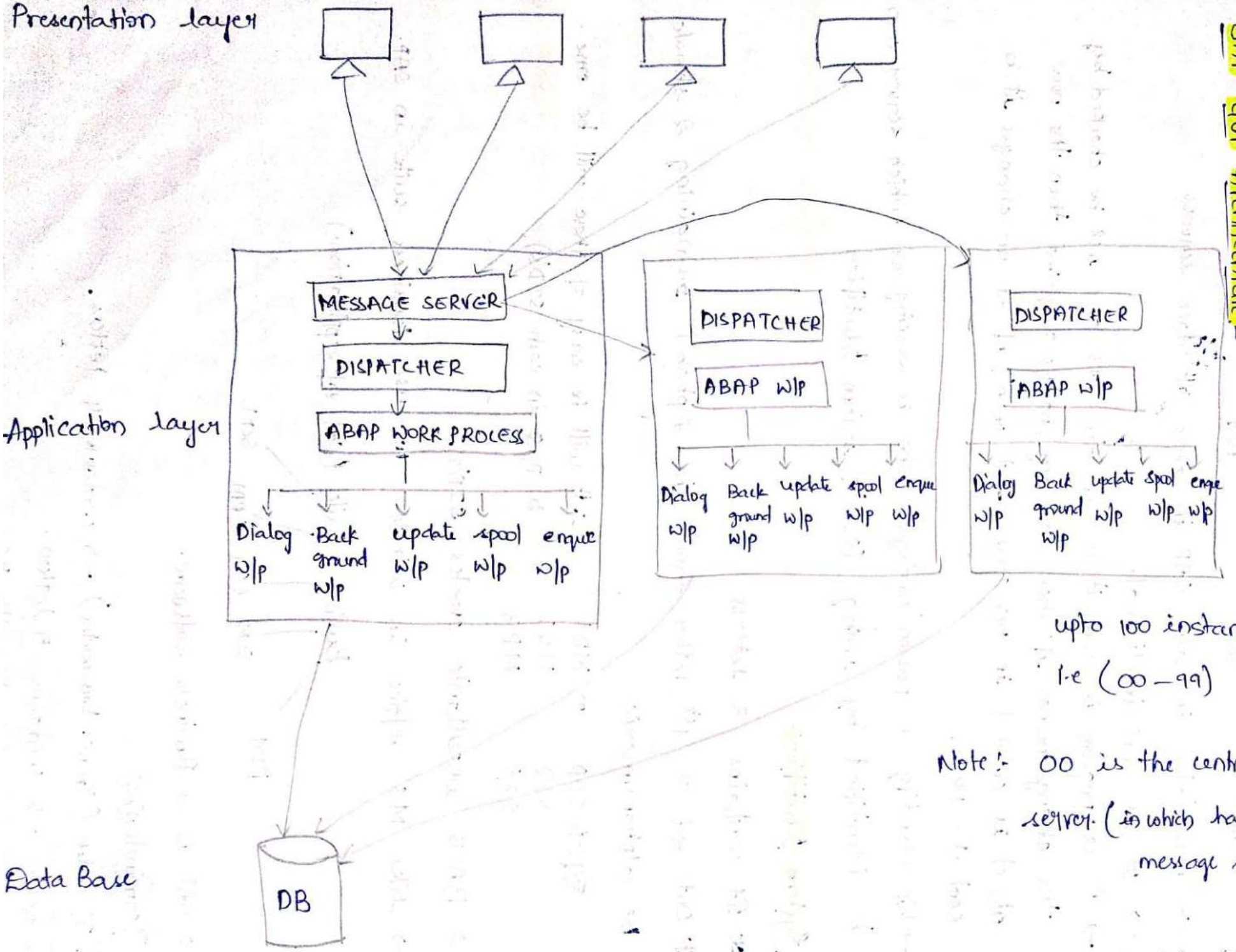
→ SAP is a Business software.

Terminologies:-

1. T- code (Transaction codes) → contains 4 letters.
2. Tables → contains 5 letters.
3. Reports → starts with RS.

→ If we want to login to SAP systems we need the above T-codes.

SAP GUI Architecture:-



execute any command is

upto 100 instances

i.e (00–99)

Note:- 00 is the central server (in which has message server).

Presentation Layer:- : Communication between user and the system.

Message server:- Receives i/p from the presentation layer and sends it to the distributed dispatcher (available dispatcher).

Dispatcher:- It takes the i/p from the message server and analyses the message (or) i/p and then sends it to the appropriate ABAP workprocess.

ABAP Workprocess:- There are 5 ABAP work processes they are as follows.

1) Dialog Work process:- It executes the user related requests (when the system is ~~in~~ logged in).

2) Back ground work process:- It updates the system at the particular fixed time (eg:- upgradation of OS, there is no need to be logged in).

3) Update Work process:- It helps to update the tables and data in the database.

4) Spool Work process:- It helps to print the data from DB.

5) Enque Work Process:- Helps to lock the tables for particular fixed time (eg:- if someone logged into the table and modifying for the particular fixed time the 2nd user cannot access that particular table i.e, it shows "table is locked") eg:- book my show).

→ There ~~are~~ 100 ~~in~~ is a limit of 100 instances but as per the company's capability there can be 2-3 dispatches (instances) as per the clients (i.e 1200, 800).

→ The difference between central system and other disp instances is "Message server".

Gateway:- Helps to connect. ~~between instances~~ acts as a bridge. 6

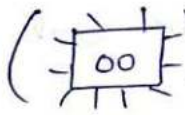
DataBase:- Stores the data in the form of (rows & columns) Tables.

Q:- How many instances do your company have?

A) 2 (or) 3 (or) 4.

* Note:- Partitioning the instances is called as client.

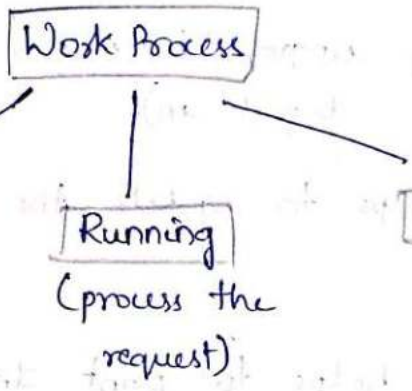
upto 1000 instances

000 - 999 (

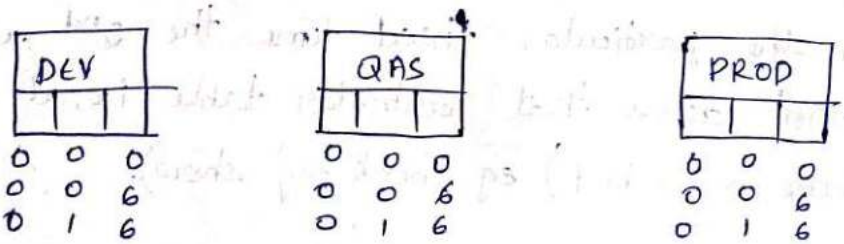
).

Example for Dialog & update w/p where both can be worked:-

If we want to update the table In the case of updating the table because user interaction & execution.



Default clients:-



000 → it is the golden client and by using this as the reference we create the new clients. (source client).

001 → Back up for the golden client (i.e 000) this can be used very sarely unless if we lose any data from 000 its a backup.

066:- Early watch client used to fix issues by raising a message to SAP people and 066 people login and resolve the issues.

→ we can create 2-3 clients and that can be any number from 000-999 (but it should be in that range. (i.e eg:- 021, 033, 234, 861, 111, etc).

ddic:- Its related to ABAP workbench and developers use this data for displaying and maintaining the meta data.

SAP default User Id's:-

	000	001	066
Sap *	✓	✓	✓
ddic (data dictionary)	✓	✓	×
Early watch	×	×	✓

(× - can't login
✓ - can login).

→ Default password for Sap * :- 06071992
ddic :- 19920706
Early watch :- support (small letters).

Note:- We need to change password in the new system as it is default password so that anybody can access that.

Flavours in SAP

IDES (used for training purpose)

Non IDES (used for Real-time purpose).

IDES- Internet Demonstration Evaluation system.

* Defaultly if we install IDE's (000, 001, 066, 800) clients are installed.

800:- Consists of sample data.

* Defaultly if we install Non-IDES (000, 001, 066) clients are installed.

Q) What are the clients installed in IDES & Non IDES?

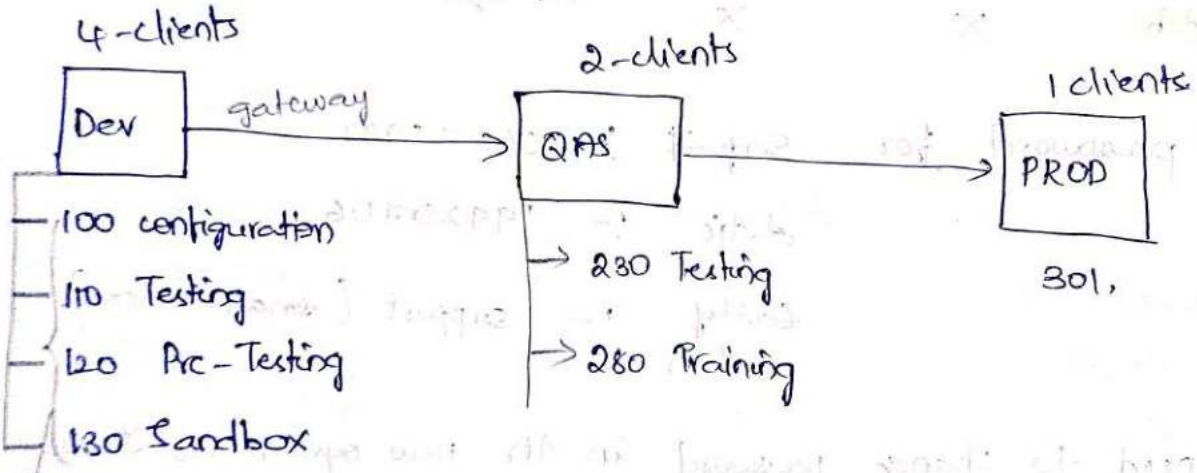
A) 000, 001, 066.

* If we want to login to SAP system using browser "Gateway" acts as the bridge between them.

* Numbers can be anything as per different organization.

* for all new clients user name is SAP * and password is "PASS" (eg:- 865 < SAP * / PASS)

↓ any number 000-999



any numbers blw 000-999

Development:-

→ Configuration:- BASIS team work.

→ Testing:- What Develop people check. (i.e in Development server).

→ Pre-Testing:- functional team will be reset it.

→ Sandbox:- Used for practice (play ground).

Quality Server:-

Testing:- Business people (change owner)

Training:- Just training (like KT) in organizations).

Powerful Profiles:-

1) sap-all :- (most powerful of all that means if any body has access then to the server then can have every data and access everything.

2) sap-new :- If there is a new patch released it wont add to sap-all until then if we want to modify anything for this new patch we should give access to the sap-new patch until it add's to sap-all.

* primarily SAP-all access should be given to ABAP and BASIS people.

* User Id creations should be in a particular format like first name followed by 1st 3 letters of the last name.

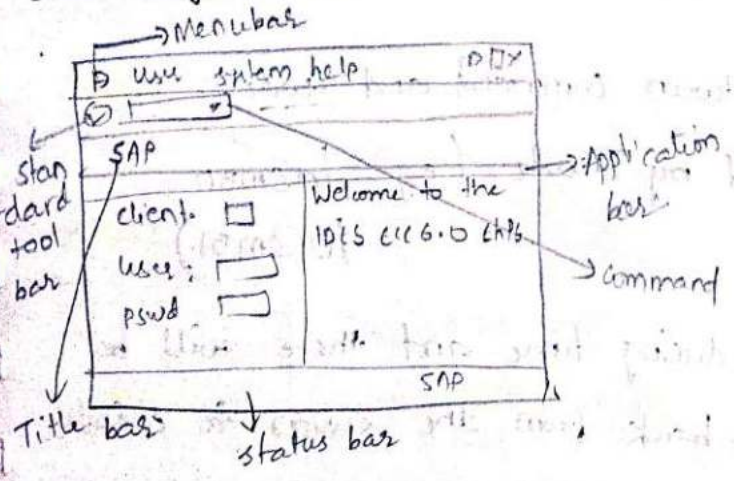
* User Id should be only 12 charecters.

* There will be only 1 Reference code from Development to production server (ie eg:- any reference numbers we get when Transcations done in bank).

9/02/2021

link to install SAP GUI :- https://sapgui.weebly.com

SAP login page :-



1) Menubar
2) Standard tool bar
3) Title bar
4) Application bar (displays after login)
5) Status bar.

Command :- T-codes are executed in this.

Note: What is SAP instance?

1) Group of services that make a system run.

Transaction Codes (T-codes)

1. SICK :- To check weather SAP is installed properly or not.
   → We execute this code only once after the installation
   → SICK - SAP Initial consistency check.
   → This is BASIS T-code.

2. SM50 :- It is used to check the status of the particular instance of the work process (ABAP work process).
   → This is BASIS T-code.

3. SM66 :- Used to check the status of all the instances of work process (status means idle, running, ended/ waiting, , abort).
   → This is BASIS T-code.

4. SM51 :- To check the status of the servers (instance), weather server (instance) is active / inactive.
   → This is BASIS T-code.

Commands:-

1) /n :- It helps to run the T-code in the same session.

2) /o :- It helps to run the T-code in new session

Eg:- Like in Google chrome there will be a option "new tab".

Note:- The should be no space between command and Tcode.

format :- command followed by T-code (eg:- /nsm50
/o sm51.)

* These commands helps in reducing time and there will be no is no need to always go back from the session to execute the new command.

Commands used to log off / logout from the SAP GUI page

1) /nend :- Dialog box asks are you sure you want to log off or not.

2) /nex :- automatically logs off.

T-codes for browsing a Table :-

1) SE16 → It shows only Table name.

2) SE16N → It shows rows & columns in the table.
   ↓
   New transaction code. * It is SECURITY T-code.

   * It is SECURITY T-code.

To generate T-code to generate Reports :-

SA38 :- Using a report it helps to check weather standard user's passwords changed (or) not.

(SA38 ↓ To generate Reports.)

Report :- RSUSR003

process to execute :- SA38
↓
RSUSR003
↓
enter.

12/2/2021

SM04 :- List of all active users for a particular instance.
It is security T-code

AL08 :- List of all active users for all instances.
It is security T-code

User Administration T-codes :-

SU01 :- Single user maintainence (i.e to create single user and can do any edits / changes for only particular user).

SU10 :- Mass / Multiple user maintainence (i.e to do to create many users and modify them).

Note:* for SU01 two fields are mandatory when we create the new user

Last name + Password.

login attempts = 6

* No fields are mandatory for SU10.

→ There are 7 icons in screen if we execute the SU01 T-code

1) Create 2) Modify/change 3) Display 4) Delete
5) copy/mirror 6) Lock/unlock 7) Reset Password.

Note:- we should not click on change always if we won't change even it shows as name who clicked.

* The length of the user id is 12 charecters

* Naming convention will be different for each organization as per their requirement

Eg:- first name + first letter in last name.

first letter in first name + last name.

Employee Id + Employ type (contract/permnant).

Q) If there is one server in the particular system how can you say wheather the server is active/inactive?

A) As we login into that particular server if it is active then only it is possible to login (always active if we can be able to login.

→ If there are multiple servers than it can be some of them can be inactive.

Tabs in creating Users:-

1) Address 2) Logon Data (contains Password) 3) SNC
4) Defaults 5) Parameters 6) Roles 7) Profiles 8) Groups
9) Personalization 10) UC Data.

* It generates 40 charecter password. (i.e we can create upto 40 charecter password (or) less).

* Note:- If some user id gets locked (ie after unsuccessful logins) we can Reset the password and should unlock the user id because it gets locked after unsuccessful login's. (i-e in Lock/unlock).

13/2/2021

* Using SU10 we can reset the password by latest version not in older version.

* Drawback for SU10:- Changes can be made for all users (like if we want to delete or modify for particular user it changes for all the users).

* SUOID :- Can display all the users and data (same as SU01 display tab).

It is security T-code.

Note:- In Defaults (tab in creating users) Output device is the Mandatory field.

* Only in Dev system powerful profiles are assigned to users.
* With a proper approvals only clearly we assign powerful profiles in production.

SUIM :- log into (i-e it monitors and has every data recorded which we ass have done) that will be displayed using this T-code

It is security T-code

SE16/SE16N
↓
USR01 :- It holds all the user master data (user master records).

~~U flag~~ SE16/SE16N
↙
USR02 :- (It holds the data of passwords of users) Logon master information.

U Flag Values:- These values helps us to know by doing which action the password has locked.

1) 0 - Not locked
2) 32 - locked Globally by administrator
3) 64 - locked locally by Administrator.
4) 128 - locked by user (by unsuccessful login's).
5) 192 - locked by administrator & user.

14/2/2021

* In SUIM we search user & Role related info.
* To browse USR02 we use SE16/SE16N.
  ↓
  USR02.
* list of users to find with starting with A* and locked by 64. using USR02.
* User lock is english name UFlag is technical name.
  SE16 → USR02 → in user (A*) & in user lock → 64
* How to extract table
  SE16 → USR01 → execute →.

User Groups:-

To create groups like & seperating the groups by category like finance department, sales etc.

SUGR → This T-code is used to create user group.

USGRP → To display the user group.

USGRP_USER → Relation ship between user group and users.

* SUPER (like SAP_all SAP*, ddic etc) is the SAP standard group. This super groups contains information related to users (like CEO's, CFO's etc.) where we cannot change their data easily.

* → This can be changed/modified if the user has assigned SUPER access

* In logon data (one of the tabs in creating users) we maintain super groups because there is authorization check.

* In Groups (one of the tabs in creating user) we create normal groups.

Creating Groups:-

SUGR → It helps to create groups.

SUIM → combination of multiple tables.

SUIM → change documents → for user.

Note:-

* Users and groups cannot be transportable from one client to other client.

* SCCS - This T-code helps to delete a client (in production) (critical T-code)

* Any thing to delete (or) modify in the production systems we need approval until then we should not do any edits.

* SM01 → This T-code helps to lock and unlock T-codes in the system.

Note: We cannot lock SM01 to SM01. in previous this the versions this can be locked by in EHP-8 package we cannot.

TSTC → To check all the T-codes in the system.

* RSAUDITC → To check the locked T-codes.

SA38 → RSAUDITC.

Note: To lock a T-code even for that we need approval.

* Using EHP they came up with the new T-codes

~~SM01~~ → ~~Dev~~

SM01_DEV → This T-code helps to lock, in the Development system and it can be transfered to Production as well.

SM01_Cust → To lock, for a time being (particular time).

* Data of log-on data is stored in USR02 table.
* Data of defaults tab is stroed in USR01 table.
* Data of Groups tab is stored in USGRP_USER.

15/2/2021 Note:

* Defaults tab the data is stored in USR01.
* Logondata tab ~~is~~ data is stored in USR02.

~~There~~ a Adding Users to groups:- There are three ways to add users to groups 1. Using SUGR.

2. SU01 → we ~~take~~ ~~multip~~ can add multiple groups to particular user.

SU01 → username → Groups → add groups → save

3. SU10 → Multiple groups to Multiple users.

SU10 → In user enter ~~ma~~ users to be created → click on create → click on change → Groups → add groups → enter.

To find U-flag values:-

1. Using SU01:- SU01 → enter user name → click on lock/unlock (displays in the dialogue box).

2. SE16N → USR02 → In user field type user name (eg:- chou-c) → execute

Multiple Users Creation:-

In Excel type users to create / Directly we can type in SU10 → copy → SU10 → paste in the user id → create.

To export :- SE16N → In table USR02 → In user type user name / no need → execute → click on export → Local file → Rich text format → enter.

Lock Multiple Users:-

SU10 → copy or type the user id's to lock/unlock → click on lock/unlock buttons.

To check the multiple users locked/unlocked.

SE16N → USR02 → In user enter fr. Value & To value → enter/execute.

Powerful Profiles:- There are 5 powerful profiles they are as follows.

1) Sap-all :- can access every thing.
2) Sap-new :- versions or patches upgrading we assign this to BASIS consultants., Basis related T-codes.
3) S_A.Develop :- We assign this to developers (ABAPERS).
4) S-A. Customiz (without e) :- These will be assigned to functional consultants (eg:- FICO, MM etc)
5) S_A : sytem :- Assign this to BASIS system.

Note:- Drawback:- If we assign this to Basis they can assign sap-all to themselves.

* These should be assigned only in emergency situations to with proper approvals (2-3 levels).

Q) How to find how many users having access to powerful profiles.

A) SUIM → users → user by complex selection criteria (the below options will be also be available in this. → profile name → sap-all (or) other powerful profiles → execute.

* To check two powerful profiles at a time to the users.

→ SUIM → user → user by complex selection criteria → same (find in drop down) → profile name (sap-all(or) any) and (sap_new*(any) → execute.

* In SUIM when we need to use change documents.

→ If it specifies any time period / date / time / modify etc.

eg:- list of users who assigned sap-all for the last 6 months.

* List of users deleted in last 6months:-

SUIM → change doumcnts → for users → from date + To date

* → scroll down → in selection criteria → we find user deleted (☑)

→ execute.

* User name who you want to ~~change~~ know that has changed, same like above but in changed by [usa name] → enter.

16/2/2021

RFC - Remote function Call.

Note:- Sap_new :- New T-codes (or) anything will be first released to sap_new after ABAPER's develop and if we give sap_all access also user cannot access to these T-codes because it is not part of the sap_all so, we assign sap_new.

Q How do we add sap-new T-code to sap-all?

SU21 → Helps to generate sap-all.

It is critical T-code.

Helps to find all the authorization data objects in the system.

* After generating sap-new object will be pulled into sap-all.

RSUSR406 :- If SU21 access has not given (critical T-code) then we use this report to generate sap-all.

SE38 (most used by ABAPERS, helps to deeply debug)

↓

RSUSR406

* We mostly use SA38.

User Group how to create :-

SUGR → Groupname → create → Text [ ] → save.

* All the user groups are stored in USGRP.

* USGRPT :- To view the text given to user group.

* Note :- 1) We find only english names in SE16.

2) We find both english (eg: user) & Technical names (eg: mandt) in SE16N

'N' indicates new Transaction code.

Deleting group using SUGR :-

SUGR → usergroup → click on delete.

Assigning one group to Multiple users :-

1) SUGR → groupname → singapor (eg) → click on modify → in users add users → save.

2) SU10 → type user names → click on modify → go to groups tab → add group name → save.

Multiple groups to one User:-

SU01 → user name → change → Groups → add multiple groups → save.

* In USGRP_USER we find how many groups has assigned to one user and how many users are assigned to one group.

SE16N → USGRP_USER → in user field type username / in user group name type group name → execute.

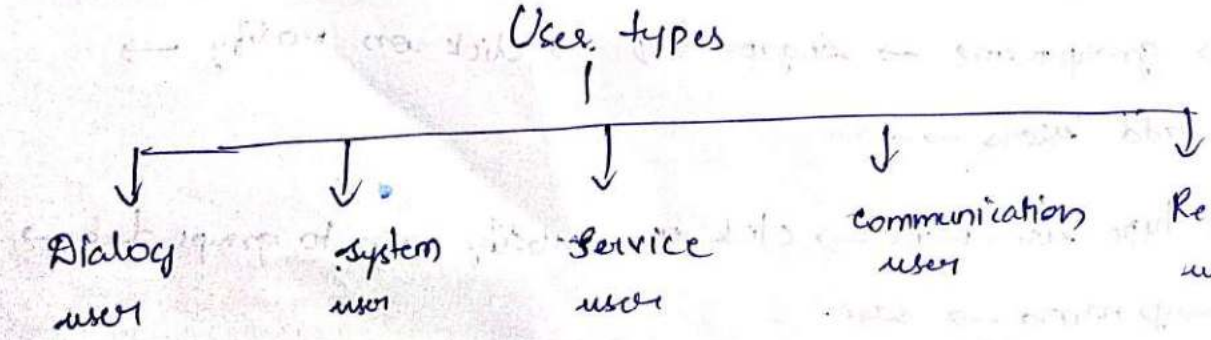
Assigning Multiple users to multiple groups:-

SU10 → enter user names → change/modify → groups → add multiple groups → save.

Note:- If some one has forgot the password (64) then the ticked will be raised then we need to check the U-flag value first as a security consultant.

* if it is 128 then unlock. we can directly unlock.
* if it is 64 then we need to ask the user get an approval from (Manager) if we recieve confirmation unlock user → Reset password → and send it to the user. (because it is locked by administrator).
* As a security consultants also we need to raise a ticket for each and everything.

User Types:- There are of 5 different types.



1. Dialog User:- All human beings comes under this 21
   → GUI login is possible.
   → Most of the users are dialog users.
   → Once GUI logon is possible
   → Password policies are applicable (i.e atleast one character should be there etc).

2) System User:- GUI If we want to schedule Background jobs then we will go for system user.

3) ~~Service User:-~~ → So password policies also not applicable
   → ~~If we want to schedule~~ GUI login is not possible for system user.

3) Service User:- Multiple user can login into the system with limited access.
   * GUI login is possible.
   * Only admin can reset the password.

4) Communication User:- If we want to communicate between one system to other system (or) one client to other client (eg: 800 to 812)
   * GUI login is not possible.
   * password policies are not applicable.

5) Reference User:- If dialog user needs extra access we create one reference user and assigned to dialog user.
   * Only one reference is added to dialog user.
   * password policies are also not applicable.
   * The relation between dialog and reference user can be seen using USREFUS.

RSUSR200 :- To check user types. (we can also find other user information).

17/2/21

RSUSR006 :- List of users ~~According~~ last to logon data and password change. it diplays user lock status also.

RSUSR007 :- Display users with incomplete address data (eg:- first name, last name, mobile no, email, etc).

SE16
↓
RSUSR007
↓
"communication person"
☑ Email ☑ lastname
☑ mobile phone ☑ firstname
↓
execute.

~~17/2/2021~~

Server
↓
100 instances
↓
Can create 1000 clients in each instance
↓
Can create many users in each client.

Creation of user types:-

1. Creating dialog User
↓
SU01
↓
user [powerstar]
↓
click on (create)
↓
Last name (powerstar)
↓
password.
↓
usertype
↓
save.

Now lets login with this user:
↓
user (powerstar)
↓
password.

2) Creating system user
↓
SU01
↓
user (sys-01)
↓
user type (system)
↓
password
↓
lastname (sys)
↓
save

→ Now lets try to login with this particular user
↓
user (sys-01)
↓
password
↓
enter
↓
logon with a dialog user

3) Creating communication user:-
↓
SU01
↓
user [com-01].
↓
user type (communication user)
↓
password
↓
last name
↓
save

→ login with this user.
↓
user (com-01)
↓
password
↓
Error
(login is not possible).

4) Creating Service user:-

↓
SU01
↓
user (service-01)
↓
last name (service)
↓
password.
↓
user type (service type)
↓
save.

log in with this user
↓
user (service-01)
↓
password
↓

Reset password is not possible (system won't change the password).

* I want to know only dialog user type:- SA38
↓
RSUSR200
↓
execute
↓
selection by user type
↓
☑ Dialog user.
↓
Execute.

*2nd method to know list of user types.

USR02
↓
user type [Dialog]
↓
execute.

5) Creating Reference User:-

↓
SU01
↓
user [Ref-01)
↓
create icon.
↓
last name (ref)
↓
user type (Reference user)
↓
password.
↓
profiles (sap_all)
↓ save.

* Assigning Reference user to dialog user

↓
SU01
↓
user (powerstar)
↓
change icon
↓
Roles Tab
↓
click on [Reference user]
↓
"REF_01" (Reference user)
↓
save.

* Now login into the dialog user:-

↓
user (power star)
↓
password.
↓
Now execute any T codes.

* Why because, if we assign reference user to Dialog user (in reference user we assign sap-all), that's why now you can execute any T-codes in dialog user (power user).

* Relationship between reference user and Dialog user can be seen in this table. USREFUS.

→ One reference is assigned to multiple Dialog user 1 Ref → 1 Dia, 2 Dia, 2 Dia

→ One Dialog user is ag assigned to one reference user 1 Dia → 1 Ref.

* To know how many dialog users are assigned to reference user,

SE16
↓
USREFUS
↓
Reference User (ref-01)
↓
execute.

X → Initial password
✓ → Indicates Initial password changed.

18/2/21

* SCC4 :- With the help of this T-code Basis consultants creates new client. and also client administration. (all modifications to client)

→ It is critical T-code.

→ The data of SCC4 is stored in the table T000.

T000 :- To find list of all clients in the system.

SE16N → T000 → execute

Note :- Deleting a client is not our task.

Locking T-code :- / unlocking T-code :-

SM01 → T-code → F4 → SCC4 → enter → search T-code to lock / unlock → SCC4 → save.

To find locking locked T-codes :-

SA38 → RSAUDITC → locked → execute

List of users having access to T-code (SU01):-

SUIM → user → user by complex selection criteria → Transaction code SU01 → execute.

* To create any user we go for SU01 & SU10.

Q) What are the things to do if employe left the organization?

A) → we won't lock the user first.
→ We supposed to deactivate the password.

SU01 → user name → logondata → deactivate password → change the validity date (valid from ↓ present date & valid through ↓ present date) → Roles (we have to remove roles → lock the user (B).

* After the audit is completed we recieve the ticket to delete the users (who left the organization).

Q How to check deleted users:-

SUIM → change diaments → for users → scroll down → delete client → execute.

* Some times security consultants recieves a ticket to copy the existing user Id's information to new user id (joined in the place of existing).. so that it is the

Q) Copying the existing user Id' to the new user Id?

A) SU01 → existing user id → copy option → from ex id + To new → check all the thing that to be copied → click on copy → logon data → Roles → Manually change the start date (because existing user id's date will be different). → logon data → change password → save.

Note:- Newly created client is stored in table T000.

Note:- for bulk users we cannot lock the users through SU10.
we have lock it for each user through SU01.

Q) Do we reset the password using SU10?

A) Still we can reset the password in SU10 now a days (EHP 7 & 8).

Illegal Passwords:-

Easily guessable passwords (eg:- Welcome, company names etc).

* User Id & password cannot be same, department names etc.

USR40:- This table maintains Illegal Passwords.

SM30:- Modifying any table using this: (we modify)(USR40). As a security consultants we will modify only that table(USR40) other will not our job.
SE16N → USR40 → execute

* Password not starting with 123 we maintain. like "123*".
* Password not ending with 123 we maintain like "*123".
* Password should not contain 123 we maintain like "*123*".
* Password should not have only Welcome but it can have Welcome123 (or) 123Welcome. it can be maintained like "Welcome".
* SAP chareters:- In SAP there are 2 charecters
  1. * (indicates full word)
  2. ? (represents single charecter).
     eg:- "shravy?" → means it should not be "shravya." (a → 7 letter. but it can be shravyay etc (8 letters))

Q) Give me a list of Illegal passwords?

A) We go for SE16|SE16N.

Q) Give me a list to modify the table?

A) SM30.

Q) Deletion of row in table do we use SM30 (or) SE16|SE16N

A) SM30.

* If we get a mail saying create a user Id shravya?

A) firstly we should check in which client we need to create the user and in i.e is in Dev, Bro, QA (system) and in which we should have SID

* SID and client number is mandatory to create a user.

Q) How do we create 5 users?

SUID (for common requirements) for same system & same department it is easy to make changes easily. for one user modification it reflects to all the users.

SUGR → User Group Administration (create user group, delete and all).

Critical Users:- SAP*, ddic, easy watch

* All critical users are maintained in SUPER.

* Execute - F8 (shortcut).

User Administration Questions:- (Home Work)

1. find the list of users in the system
2. find the list of users who has not logged in to the system since 90 days.
3. find the list of system users who are valid today.
4. find the list of service and communication users in the system.
5. find the list of reference users and the dialog users to whom the reference users are assigned.
6. find the list of users locked by Administrator.
7. find the list of users who are having access to profile SAP_ALL?
8. How do you ensure that only reference users are assigned to dialog user?
9. find the list of locked Tcodes in SAP?

10. Find the list of users who have logged in to the current instance?

11. Find the status of the server?

12. Find the list of users who still have initial password?

13. Find weather SAP is installed properly or not.

14. Check weather the standard user's passwords are changed or not?

Powerful Profiles Questions?

1. Find the list of users having access to the profile SAP_all?
2. Find the list of users having access to the profiles SAP_all and sap_new.
3. Pick the first user in the list of users having SAP_all and find out who has assigned SAP_all to the user.
4. Find the list of Users having access to S_A. system.

SM25 :- This T-code helps to lock all users.

SM25 → choose user → lock/unlock ☑ → save.

* We won't perform this at all.

Modifying USR40 table using SM30:-

SM30 → Table/view USR40 → click on Maintain → Caution: The table is cross client (client independant) → click on continue ☑ → click on new entries → type at Paword Patt./Indiv. value (eg:- * shravya *) → case sensitive ☐ → save → click on (☐) → type short description → save.

* If we check ☑ in case sensitive system will only accept "CAPITAL" letters.

* If we uncheck ☐ in case sensitive systems will not accept either caps or small notes.

Data

Client Independant | client dependant

***

Client Independant:- If we make any changes for particular client (800) it reflects for all the other clients.

Client Dependant:- If we make changes for particular client (800) it reflects only to that client (800).

Note:- Mandatorily we need to give short description.

System Profiles (Defines behaviour of your system).

Start | Default | Instance

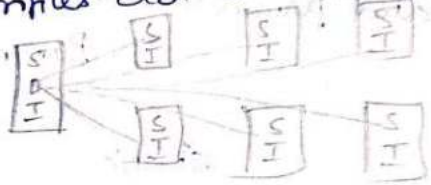
Start:- It defines how SAP should start/stop. will have some instructions.

Default:- If we change for 1 instance it effects globally for all instances.

Instance:- If we change for 1 instance it effects locally for that particular instance.

Q) I have 60 instances how many system profiles do we have?

A) 121 (i.e start 60 + Default 1 + Instance 60)
= 121.



* Note:- 1) If we change a value for the parameter it only reflects after the server restart in "static". (it won't reflect immediatly).

2) Dynamic:- If we make changes it will reflect immediatly.

RZ10 :- It This T-code helps to change the parameter values (eg:- pswd length = "6").

RZ11 :- This T-code helps to check the information of parameters (eg:- password validity = '30'
↓
represents days/month/year will be known by RZ11).

* Note:- In latest versions "start" is merged into "Instance".
(EHP, 7 48).

Q) Change Password length = 10.

A) RZ10 → profile [ ] → click on → select profile name (eg:- EH7-DVEB MCS99 - ECCEHP97)
→ select extended maintainence →

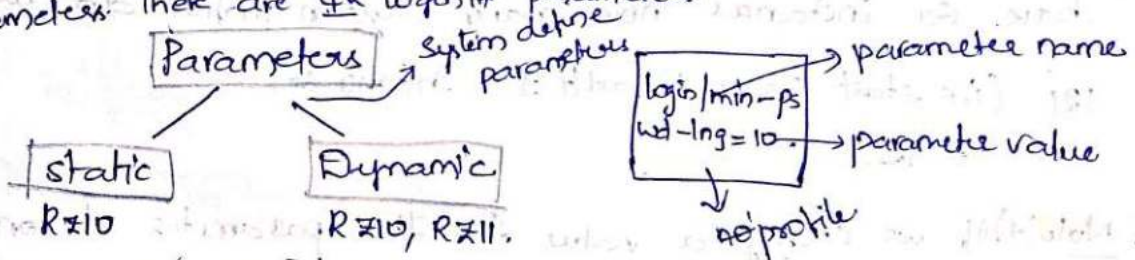
Deleting an illegal password:-

SM30 → Table/view [USR40] → Maintain → caution:- Table is cross-client → click on ☑ → select row (pswd) you want to delete → click on 🗑 → edit save → click on ☑ → save.

Changing Password length to 10:-(Defaultly pswd length should be '6').

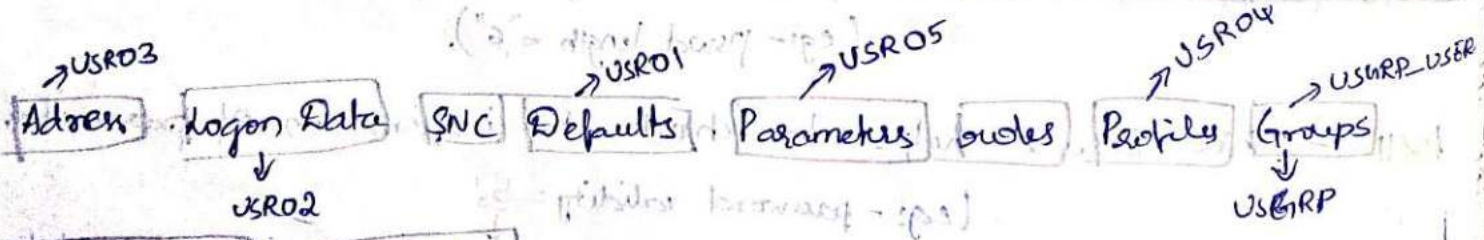
RZ10 → profile [ ] → click on → select profile name (eg:- EH7-DVEB MCS99-ECCEHP97) → select extended maintainence → create parameter (click) → parameter name (select) by (login/*) → select login/min_password_lng → parameter value [10] → copy → (after version is increased by 1 (eg: 52-53).

Note:- To check the/find the parameter name search as (login/*)/pswd related parameters. There are 42 login/* parameters.



find description for login/min_password_lng (parameter length):-

RZ11 → Parametername → select parameter → by login/*) → click on Display/ Display Doc



Note:- Based on the our instance profile we need to select the profile (in parameters topic).

Password policies:- (Home Work by Rakesh Sir)

1. There should be atleast three different charectors compared to old password while creating new password.

A. parameter used to this :- login/min_password_diff

2. There should be atleast 2 special charectors in the password.

A: parameter used to this :- login/min_password_specials

3. Password should expire after three months of creation.

A. parameter to be used :- login/password_expiration_time

4. There should be atleast 2 numbers.

A. parameter to be used :- login/min_password_digits.

5. There should be atleast 2 lower case letters.

A. Parameters to be used :- login/min_password_lowercase

6. Length of the password should not exceed 10.

A. parameter to be used :- login/min_password_lng.

User Administration Questions:- (Home work by Raja Sir).

1. find the list of users in the system?

A:- SE16N → USR01 → remove maximum number of hits → execute (6,508).

2. find the list of users who has not logged in to the system since 90 days.

A:- SE16N → USR02 → In last logon time enter the value of To value (19/1/2020, 19/2/2021) → execute (3809).

3. Find the list of system users who are valid today?

A:- SA38 → RSUSR200 → users valid Today → system user → execute (29)

4. Find the list of service & communication users in the system?

A: SA38 → RSUSR200 → user valid Today → service & communication user → execute (1,090)

5. Find the list of reference and the dialog users to whom the reference users are assigned.

A) SE16N → USREFUS → execute → (6509)

6. find the list of users locked by Administrator?

A. SE16N → USR02 → In user lock type [64] → execute (266)

7. find the list of users who are having access to profile sap_all?

A) SUIM → User → User by complex selection criteria → profile name [sap_all] → execute → (329)

8. How do you ensure that only reference users are assigned to dialog user?

A) Because no other user is assigned except reference user/USREFUS

9. find the list of locked T-codes in SAP?

A) SA38 → RSAUDITC → execute (0).

10. find the list of users who have logged into the current instance

A) SM04 → enter → Logon list of server ECCEhp7_EHP_94

11. find the status of the server?

A) SM51 → enter → (active)

12) find the list of users who still have initial password?

A) SA38 → RSUSR200 → execute → (1,612)

13) Find weather SAP is installed properly(os) not?

A) SICK → enter → no errors reported.

14) check wheather standard user's passwords are changed or not?

A) SA38 → RSUSR003 → execute (43)

Powerful Profile Questions:

1. Find the list of users having access to the profile SAP_all?

A) same as 7th answer (330).

2. Find the list of users having access to the profiles sap_all and sap_new?

A) SUIM → User → user by complex → profilename [sap_all], AND Profil. [sap_new] → execute → (257)

3. Pick the first user in the list of users having sap-all and find out who has assigned sap-all to the user? 33

A) Picking the first user:-

SUIM → users → use by complex selection criteria → profile name [SAP_ALL]

→ execute → [4A9]

Who has assigned sap-all to the user

SUIM → change documents → for users → user [4A9] → scroll down →

check all the attributes → execute → (Rikshitol)

4. Find the list of users having access to S_A.system?

A) SUIM → user → use by complex selection criteria → profile name [S_A.system]

→ execute → 13) (STABEL, WF-BATCH, WORKFLOW)

20/2/23

* Login parameters are called as system parameters & system behaves based on the parameter given.

System related Parameter Reports:- T-code

1. RSPFPAR :- This helps to search a particular parameter.

To remember it RS PF PAR → parameter,

Report, profile

SA38 → RSPFPAR → Profile parameters [login/min_password_lng] → execute.

2. RSPARAM :- This Report helps to search for all parameters

SA38 → RSPARAM → execute. TPARA: List of Parameters.

Protecting SAP* against misuse:-

* For SAP* with password 06071992 we change the password mandatorily.

* But for SAP* with password "PASS" as we can won't change the password it can be accessed easily so that for protecting it from misuse we ~~use~~ p maintain parameter.

* The values for this parameter login/no_automatic_user_sapstar are 0 & 1.

0 - indicates user can access with this sap* if we provide this parameter value

1 - indicates user cannot access sap* if we provide this parameter value.

* This parameter can be set by using the T-code RZ10.
* BASIS consultants use this SAP* with password "PASS" to login into SAP.
* This is like if BASIS people want to create a client he need to login through SAP* & password "pass" not through SAP* 06071992.

Note:→ Anybody can access SAP* with password 06071992.

→ But if we restrict SAP* with password "PASS" nobody can access it.

* There is no provision to restrict SAP* with password as "PASS" so we maintain it with parameter to restrict is

login/no_automatic_user_sapstar

RZ10 → Create parameter → profile [ ] → extended maintainence → current version 000 with current instance 99

change → create parameter → Add parameter name [ ] → value [ ] → copy → click on back button → copy → click on back button → save.

Note:- Every time if we change any parameter version value will be increased by '1' (eg 50+1, 51).

Some important point related to clients & default users:-

* When we install SAP clients are created by default 000, 001, 066.
* If we want to login into any standard client we login through users sap*, ddic, earlywatch.

Q) Password policy will be client wise (or) system wise (or) user wise.

A) System wise (i.e for entire server (or) system it will be same).

Secpol:- This helps to maintain specific policy to some main users.

→ This applies for user level.

Q) Secpol → New Entries → Security policy [Basis policy] (can be any name as per requirement), Password Policies for basis consultants (description) → Attributes → choose attribute name [ ], value ( ) → save. (If sequent has not created enter short Description [ ] → ↵ new entries)

as per the requirement of organization.

* We have to maintain/provide a policy name.

Assigning secpol policy to a user:-

SU01 → Logondata → security policy [Basic policy] → save.

Checking the user who has provided by secpol policy:-

SUIM → change documents → user [ ] → [✓] security policy → execute.

* Some times if we couldn't know the user name in changed by provide [*].

SUIM → change documents → for user → changed by [*] → [✓] deleted user (after scroll down) → execute.

Q) If the password length in default profile is 8 and the password length in Instance profile is '7' what will be password length to user.

A) Instance '7'

Instance
Default
Sifart

(As the it is layered the top will be instance and the length in instance is the length for user).

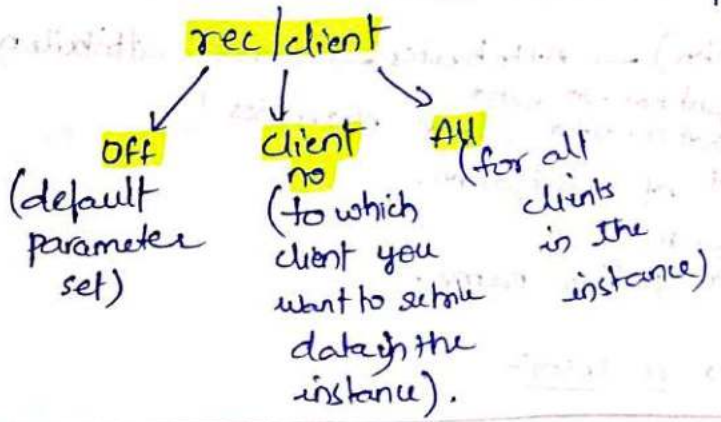
Q) What if some user it has a problem logging in it seeps and comes & raises a ticket to security consultant? (Uflag value '0', correct credentials provided).

A) He might be logging into different SID & different client (eg:- Hitachi).

right SID, right client weather he is logging in with these we need to check for first.

21/12/21

1. **Rec/client**: It is a static parameter and it helps to find the data who has modified in the tables like ABAPERS and security consultants (we only modify the table USR40 (password parameters)) to know who has changed and when has changed/modified. The table this ~~re~~ these prerequisites helps to ~~find~~ retrive them. with the help of two pre-requisites rec/client & SE13.



RZ10 → profile [ ] → extended maintanence → change → parameter → create parameter → parametername [rec/client] → value [ ] → copy → back → save.

particular client (or) clients upto '10'. / All.

2. From which table should we need to ~~retrive~~/see the log records;

* As the security consultants we only use/modify the table USR40 with the help of SM30.

SE13 :- ~~From~~ To This ~~T-code~~ helps ~~from~~ ~~which~~ ~~table~~ ~~to~~ retrive data from ~~the to~~ choosed ~~table~~.

SE13 :- This is the 2nd prerequisite. This t-code used for maintain Technical setting (Tables) in SAP.

SE13 → Table/View [USR40] → change/Display → ☑ log data change → save.

* After the modification in table USR40 by SM30.
* Logged data is activated is done by SE13.

* To retrive data which has modified by whom:-

SCU3 :- This t-code helps to retrive data.

SCU3 → evaluate logs → Table USR40 → static data Previous data →
Tables ⊙ → execute.

* SE16A → DBTABPRT :- helps to retrive data, log records are stored in this table.

SE16n → dBTABPRT → USR40 → execute

* SE DBTABLOG :- helps to retrive data, log records are stored in this table.

SE16n → dbtablog → USR40 → execute.

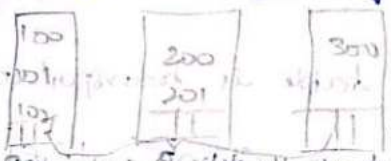
Note:- Mainly we use SCU3 to retrive data.

USR03:- User Adress Information. (This table holds user address information).

22/2/21 Rakesh sir class

Detailed information about SCC4:-

→ As this help t-code helps to create clients by BASIS people not only this it Tcode does helps to modify/exchange any information for the client. i.e client administration.



* In Development system clients are modifiable
* Users are client dependant.
* MANDT (clients) are client dependant.
* We can restrict modifications for particular client by SCC4 and for entire system also we can restrict the modifications. And if it is restricted for entire system and want to modify for the particular client it is not possible.
* for one system we change for only one client.
* Client opening and closing will be done by security consultant.
* USR40 is client Independant.

Note: Users are not transportable from one system to other system.

* Client Independant (Repository) (RIN- Repository is independant)
* client dependant (customizing data)

SCC4 → change/display → Caution: The table is cross-client ☑ → double click on client which you want to give modify changes → client role [select appropriate] one which system you want to modify → below we have to select appropriate dropdown as the system (Dev, Qu, Pro) → save.

eCATT - extended Computer Aided Test Tool. (tool for software test automation developed by SAP. offers a graphical user interface with ABAP script editor and its own command syntax.

Note: Tooo is a very critical client there is a chance to delete a client.

Note:
→ The moment we make a change the transport request will be generated it records using transport export.

* USR40 table is transportable.

Q) Options in Client role Specific?

A) 1. changes without automatic recording.
2. Automatic recording of changes
3. No changes allowed.
4. changes w/o automatic recording, no transports allowed.

SE06:- This t-code helps to modify system Globally. → Global settings

Note: client opening and closing will be done by security consultant.

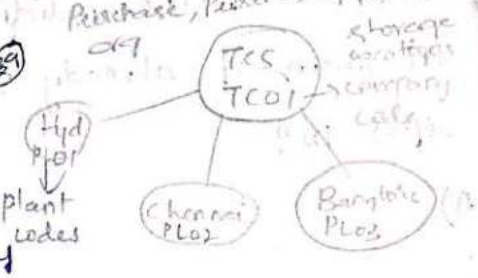
SE06 → Global Setting → [Modifiable]

How do we open a client:-

SCC4 → select client → change/modify → client role [customizing]

TOO1 → This t-code helps to know about the company codes of finance department.

→ This is very critical code Table.



TOOIW → This t-code holds/gives the data/details of company plants, Branches.

→ This is very critical code Table.

TOOIL → This t-code holds/gives the data of storage locations of companies

→ This is critical T-code Table

MARA → This T-code gives the information of the material of the company.

→ This is critical table.

MARD → This table gives the information of storage location of material, This is critical table.

MEAIN → It is a transaction code used for Create Purchase order in SAP., this is technical data table.

Note:- 800 client should not be created in Non-Ides.

Technical names for below:-

1. Company code - BUKRS
2. Purchase Org - EKORG EKORG
3. Purchase grp - EKGRP EKGRP (
4. plant code - ~~BWKEY~~ WERKS WERKS (TOOIW)
5. Storage location - LGORT (TOOIL) LGORT (TOOIL)

23/2/23 (Rakesh Sir class):-

Note:- User groups are not - transportable

Q) What is an Organization structure?

A) A 3 landscape mode is organization structure (Dev, Qu, Prd).

Q) What if the validity of the user ended today? i.e. What happens at 12am if already logged in and what happens if he tries to login after 12?

A).

Note:- In real time we run scripts rarely

* ECATT:- To create user id's in mass level (eg:- 1000) then we don't create it manually, we maintain all the users and details in the excel sheet and then run ECATT as it script so that users are created as per the requirements with the proper approvals (we run ECATT script). N- In real time rarely we run this script.

SE37 :- Not to This t-code helps to restrict/unrestrict to login to particular client (lock/unlock client).

SE37 → Function Module [SCCR_lock_client/SCCR_lock_unlock_client] →

execute → client [ ] → execute
↓
select client

* Functional Module: SCCR_lock_client (to lock client)
SCCR_unlock_client (to unlock client).

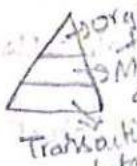
Q) What if you login to same client & lock the client?

A) By using RFC we can login to other client & lock the client (which client to be locked).

* Master Data:- This Data won't change regularly.

Transaction Data:- This changes regularly (transactions, credits, debits, Materials etc).

4-eye principle:- The master data is checked twicely. before after the changes.



ME22N - This helps to change the Purchase Order (after the creation of PO).

ME23N - This helps to display the purchase Order.

Sales Department:- sales org
shipping point
Distribution channel
Division
Sales Area

VA01 – This t-code helps to create sales order
VA02 – Cha This t-code helps to change sales order.
VA03 – This t-code helps to Display sales order

Q) What if client says to give access as you wish?
A) We should assign Display access to the client.

Q) What if we want to create purchase order for plant SOHY & SOMU. (2) (all) (1) ↓ Mumbai ↗ hyderabad
A) We have to create two purchase orders seperately in this case.
(SOHY (*) & SOMU (out of 2 should create 1)).

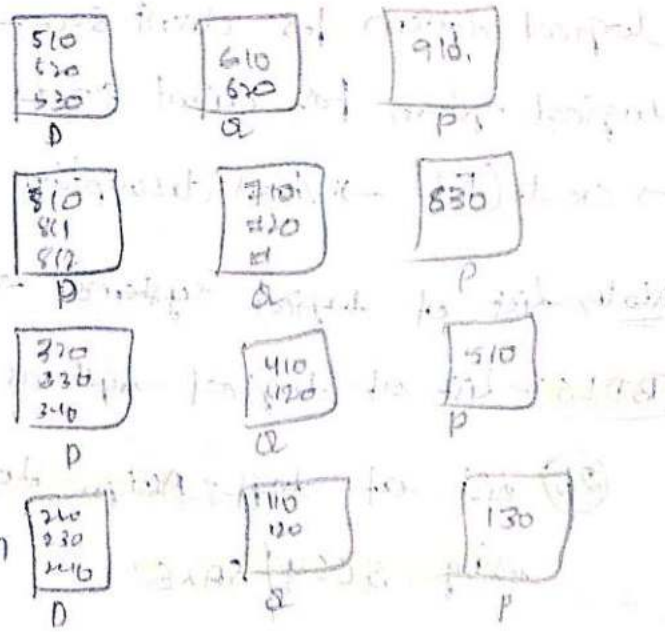
Note:- We have to maintain value madatorily we should not leave it empty.

Note:- *(value) indicates all.

24/2/21
☆☆☆

CUA – Central User Administration:-

* Firstly we need to understand the organization landscape. ~~first~~.
Note:- Same clients can be exists in other landscapes but not in same landscape
* Instead of logging into the each client to create users (bulk users) as it is much time taking consumes much time ~~if~~ this CUA helps to create users from one client (parent) to all other clients (child clients).
* User administration ~~takes~~ tasks can be done.



* We have to follow the following steps to achieve CUA.

(1) Choose which system is parent system and which one is child system. This is the task for Security Consultant.

Eg:- out of 30 clients one is parent & remaining 29 are child.

(2) Create logical systems for all the clients and assign logical system to appropriate client. Task for BASIS consultants.

Logical System :- It uniquely identify your client across the landscape.

(2a) BD54/SALE :- If we want to create logical system to client: this is the t-code we use.

Naming convention for creating Logical System:- <SID>CLNT<client.no>

eg:- D40CLNT145
SID client.no.

RSUSR003 - To check whether standard user pswd changed or not.

Consider & choose parent system → 800
child system - 810.

→ Create logical systems to parent as well as child. systems using BD54/SALE.

Naming convention for client 800 → DH7CLNT800

Naming convention for client 810 → DH7CLNT810.

BD54 → crossclient (v) → new entries → log systems = DH7CLNT800 → Name logical system for client 800 → log. system = DH7CLNT810 → Name logical system for client 810 → save → Prompt for workbench request → create (F) → short description → save.

~~Note:- List of logical systems can be seen in table TBDLS.~~

TBDLS:- List of logical systems can be seen.

(2b) dist of logs - Assign logical systems to appropriate clients using SCC4/SALE.

SCC4 → click on display change → cross client ☑ → double click on particular client (eg: 800) → Parent → logical system DH7CLNT800 → save → Double click on (eg: 810) → child → logical system DH7CLNT810 → save (42)

(3) Create communication users for both parent as well as child clients. (systems) and assign defaults roles to communication user.

* This is the one time task. (security consultants task).

Note: We create only one communication user for Parent client but we create communication users for all child clients (i.e to obtain connection between parent & childs).

3a) Assign Default Roles to parent system communication user.

- SAP_BC_USR_CUA_CENTRAL → indicats for parent (central).
- SAP_BC_USR_CUA_CENTRAL_BDIST
- SAP_BC_USR_CUA_SETUP_CENTRAL.

SU01 → user CUA-USER → create → last name CUA-PARENT → Logon data → set to communication user (drop down) → Password setting → Roles → SAP_BC_USR_CUA_* → find (🔭) → search → select ( ) → save.

~~How~~ → 3b) Assign defaults roles to child system communication user.

→ Create child system communication user : CHILD_CUA - child system client is 810.

→ To create we need to login in to 810 (child) client. Assign default roles to child system.

- SAP_BC_USR_CUA_client → indicates for child (client).
- SAP_BC_USR_CUA_client_RFC.
- SAP_BC_USR_CUA_SETUP_CLIENT.

Login with 810 (sap* pswd 060719921 (or check in Report RSUSR003 weather the pswd sap* is well known for 810.)).

→ SU01 → user child-CUA → logo create → last name child → logon data → password set → Roles communication user → Roles → SAP_BC_USR_CUA_* → find (🔭) → select → (✓) → save.

(4) Create RFC connections between PARENT(800) to CHILD(810)

Basis task.

↓

Remote function Call :- To connect one system to other (or) one client to other.

CHILD(810) to PARENT.(800).

PARENT to PARENT (dummy (optional)).

Parent (800) ~~to child (810)~~ ~~to~~ Parent (800) to child(810)

SM59 → To create RFC (it is bidirectional).

SM59 → create (F) → RFC Destination (to maintain destination related logical system name:) DH7CLNT810 → Connection Type 3 (connection to ABAP system)

→ Description Parent 800 to child 810 → logon Security →

Language EN → english

client 810 → save → connection Test utilities → Test →

1. Connection Test
2. Authorization Test.

user child-CUA

password welcome123

Child (810) to parent (800) :-

SM59 → RFC Destination DH7CCNT800 → description child 810 to parent →

Connection type 3 → logon security → language EN → english → save →

client 800

user child CUA-USER

pswd Welcome123

test → utilities → Authorization Test

Connection Test.

Security consultant.

(5) Attach all the child systems to parent systems. using SCUA :-

SCUA → Model view (modify use Y & Z) YCUA → create → sending system (default given) DH7CLNT800 → Table (Recipient → DH7CLNT810, SAP system EH7, client 810 → Basis SP → save.

Note:- Now CUA is ready we can create users from central system. to all choosed system. (no need to login to each client to create users).

→ If you can't find create tab it is child system.

→ System tab is found in Parent system. (so that we can identify that it is parent client/system).

Creating User for child (810) using Parent (800):-

SU01 → user [coffee] → lastname [coffee] → [redacted] [Pswd] → systems

(Recurring system → find → select particular client (810) → DIFFCLNTE10 → save.

How to delete CUA configuration:-

RSDE2CUA → To delete CUA configuration we use this Report.

SA38 → RSDELCUA → uncheck Test ☐ → Delete → complete CUA ⓒ → execute.

Rakesh Sir class: ★★★

Q) Before Purchase Order creation what is the Prerequisite.

→ Request for a quotation.

Purchase Request :- This can change.

Purchase Order :- This cannot change.

Material Requirement Planning.

vendor1 vendor2 vendor3.

RFQ → Request for quotation.

(R1) → Purchase Order – clerk

↓

restrict for which (as per requirement)

clerk

HYD (HY10) MUM (MU10)

Activities:- 01 (create), 02 (change), 03 (display), 04 (print), 05 (lock/unlock/reset pswd), 06 (delete), 16, 22 → enter, include, assign., 60, 61 → export → import, 43 → release.

★ → indicates all access granted.

TACT → All activities are stored.

Note:- To execute purchase order we need to assign 16 - Activity.

→ To assign a role we need to have 22 activity.

→ To assign a role for create should give the activity value 03.

→ Authorization objects will have mostly 2 fields minimum fields should have is 1 maximum is 10.

Hierarchy in Security:-

Object class (OC)

↓

AO (Authorization object)

↓

Fields (Maintain Values)

* Based on different functional modules like (MM, FICO) we use other Authorization objects like

(46)

S_user_GRP → security.
F_user_GRP → finance.

Role Owner: Checks weather activities given to users correct or not.

SU01 → Role assignment → S_USER_GRP (AO)

↓

Two fields

Class [Aus]

Activt [01, 02, 06]

Eg- GUCCI

Plants: Aus, US, GER, ITA

Bharu, Anjali, Shravya, Vani

(1 role is enough for one country)

Z-UA_GUCCI_AUS

* Technical name for class is User Group.

⇒ Shravya should have 3 roles. (3 times authorization)

Class [AUS] class [US]. class [GER]

Activt [06] Activt [01, 02] Activt [03].

S_user_Grp +1 +1

S_user_pro (profile) → Profile tab is controlled.

profile name [ ]

Activity [ ]

S_user_Grp → controls 7 tabs in groups.

Q) Sunny should not have SAP_all profile.

1st step use S_user_group and step S_user_profile

class [AUS] & profile [sap_all]

Activ [01, 02] Activity [01, 02, 22]

Q) Expect sap_all we need all profile access

1+1+S_user_profile.

profile [A* → SAP_ALL; SAP_ALM → Z]

Note: ***

* If the clerk get replaced then we [COPY] the same roles to the new one (we wont always ask for approval (SS) create new roles).

* We don't create roles for the new user every time.

25/2/21 Rakesh sir class.

P-P (Procurement cycle).

ME51N – Purchase Request (Requisition).

ME52N – Helps to change Purchase Requisition.

ME53N – Helps to change Display Purchase Requisition.

→ RFQ – Request for Quotation.

ME41 – Helps to create Request.

ME42 – Helps to change Request.

ME43 – Helps to Display Request.

MIGO – Helps for goods Movement in SAP.

ME28 – Helps to Approve PO (Purchase Order).

ME45 – Release RFQ.

PFCG – Helps to create a Role.

PFCG → Role → Z_BEAM_QUATATION_VENDOR_CLERK → single role.

↓

should start with 'Y' or 'Z' (Helps to identify these created manually).

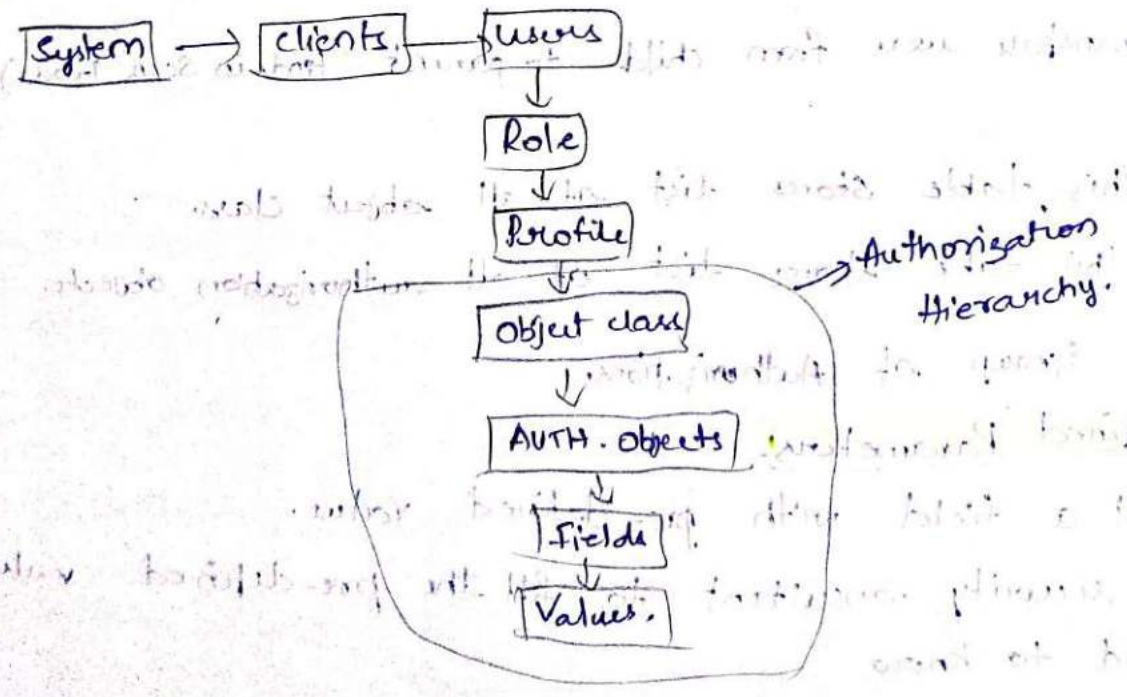
Raja sir class

CUA – One Parent three Childs:-

→ ~~Same as One parent one child two provide all the rules~~

Same process as One parent one child.

Security Hierarchy:-



Role :- Job description of an employee in an organization. (4/8)

Profile :- Group of authorizations.

Object class :- folder.

* Roles are of no use without profiles.

Q) How can you identify authorization Object :-

A) Module name followed by '_' (underscore).

Eg :- SD → 'V_', MM → 'M_', HR → 'P_', ABAP/BASIS/security → 'S_'

F → 'F_'.

Different types of field names :-

1. Globally
2. local
3. Proposal.
4. Redist
5. Evrywhr (Every where).

SCUM :- Where you maintain field parameters (maintains tabs in SU01)

SCUG :- To transfer child system users to parent systems.

Note :- These T-codes will execute only when CUA connection is available

SCUL :- Helps to generate locks (CUA).

SU01 → Transfers users from child to parent (finds in SCUL T-code).

26/2/21

TOBC - This table stores list of all object class.

TOBJ - This table stores list of all authorization objects.

Profiles :- Group of Authorizations.

***

User Defined Parameters :-

→ To fill a field with pre-defined value.

→ As a security consultant to fill the pre-defined values we need to know

→ We need to know the parameter Id for that particular field.

→ At the field right click □, then click on help. You'll find (symbol of hammer+) Technical info tab click on that you'll find the parameter Id for that particular field and copy that particular Id.

USR05 :- Relation ship between Parameter and users can be seen in this table

Example: VA01 → sales organization field should be UK

VA01 → sales organization [ ] → Right click → help F1 → click → parameter Id VKO → copy Id → SU01 → user composit → change → Parameters → Parameter Id VKO → value UK → save

→ To check login with UId composit and try to execute T-code VA01 you will find the user defined parameter UK in sales organi-zation field.

End User Transaction codes:-

These are used when some user want to change his/her user defined parameters (eg. location changes) by the help of these T-codes these parameters gets modified.

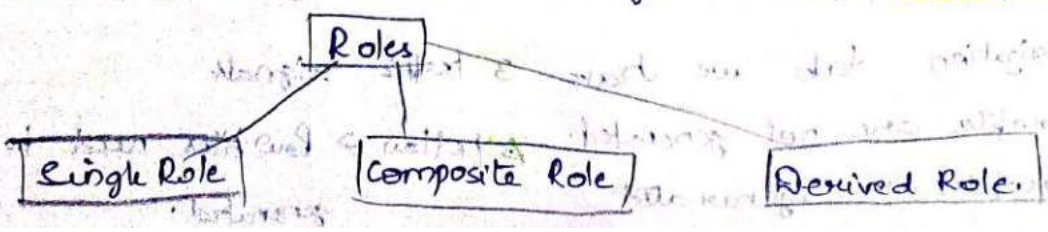
SU0 → User can Modify default values

SU1 → user can modify address info.

SU2 → user can modify parameters info.

SU3 → (SU0+SU1+SU2) → users can modify default values, address info and parameters info.

Note :- Important T-codes for security consultant. SU01 & PFCG.



Note:

* Role and Single Role are same.

① Single Role:

→ There is no provision we directly assign T-codes to the users. Instead we create a role, add transaction-codes to role and assign it (role) to the user.

→ for single role we use 'Z' (to differentiate btw composite & single Role) as there is no role) but ".

→ for composite role we use 'Y'

→ The naming convention will be different from organization to organization.

Q) How to create a Role:-

A) PFCG → Role [Z_BMW-SEC-SECTION] (can be ":") → click on single role → Description field [BMW_SEC_consultant_role] → Description (down) → copy Ticket info / Mail paste → click on Menu Tab → click on Transaction → Add SU01 T-code → Assign Transaction → Authorizations → scroll/down → click on change authorization data → To view technical names → utilities → settings → ☑ show Technical Names → save ☑ → click on generate ⊗ → profile names are created → continue → Back.

Q)

Note:- Tabs in PFCG

1. Description 2) Menu 3) Authorization 4) User.

* Red & Green & Yellow ~~doors~~ colours are called as Traffic signals.

* Technical name for T-code is TCB.

→ In menu tab Red 'O' indicates T-codes are not added.
In menu tab Green 'O' indicates T-codes are added.

→ In authorization tab we have 3 traffic signals

O Red → Profiles are not generated. △ Yellow → Profiles need to be generated.

□ Green → Profiles are generated

→ In user tab we have 3 traffic signals.

'O' Red - Users are not assigned.

Green - Users are assigned.

Δ yellow - Users need to be user comparision.

Note: Don't click on save after go the Role 'Generation ⊗

* Assigning roles to users ; 1st user - ☆ , 2nd user - only some activity values

* All buttons in SU01 maintains by Authorization object

S_User_GRP — Activt
class.

→ AAAB (object class).

Eg:-

Senior security Consultant:-

PFCG → Role [Z_bmw_sec_srsecon] → single role → Description [sr sec consultant code] → Menu → Transaction → SU01 → Assign T-code → click on Authorization → ☑ → expand standard → click on expand (S_User_grp) → Activity [01, 02, 03, 22 / full authorization] → user group [class] → Generate → ☑.

Assigning roles to Users:- using SU01:-

SU01 → user [srsecon] → lastname → logon data → pswd → Roles → Z_Bmw_* find → select the appropriate role [Z_bmw_sec_srsecon] → save.

Assigning roles to users using PFCG:-

PFCG → Role ☐ → change → users → userid. [JRsecon] → user comparision → complete comparision.

Note:→ from SU01 we can assign multiple roles.

→ from PFCG we can assign multiple users for roles.

* Restrict a user by 'Authorization' objects, fields and values using roles.

→ To restrict Roles tab we have Auth-object S_USER-AGR

ACTVT, Rolename → fields.

→ Profile authorization object S_USER-PRO

ACTVT, ProfileName → fields

→ We cannot assign directly profiles to the users, so we use Roles.

Q) Does Role exists without a profile?

A) Yes, But of no use.

Q) Does Profile exists without a Role?

A) No.

(2) Composite Role: To avoid Multiple single roles assigning to users we combine the single Roles and assign these roles to composite Role. By this the composite Role is assigned to the user so that he can have multiple access. And time consumption is less. It is a critical Role because assigned access will be given to user.

PFCG → Role Y_ICICI_Vice_In_Main → composite Role → Description

Roles for vice president 2nd → Roles → assign → two single roles → Menu

→ Import menu → Assign roles to user → SU01 | PFCG

SU01 → Roles → assign composite Role

PFCG → users → avid name.

Note: We cannot assign composite role to composite Role.

→ We don't find authorization tab in composite Role.

→ We find "Roles" tab (extra) in composite Role.

→ We can't assign profiles in composite role.

→ Activ column helps to Active ☑ role (or) Inactive role.

* for example, if a user doesn't need access of 1 role for 20 days then we can uncheck that particular role in Activ ☐ in composite role instead of deleting a role. (83)

Q) How many single roles can be assigned to composite roles.

A) 'N' number of roles (but in real time we wont assign much)

Agr_Users:- This table helps to show ~~what~~ list of ~~are~~ the users assigned to the role.

Note:- Standard profiles can be exists / provided without a Role. (Internal purpose)

Q) What happens in the background when we add T-code?

A) 1) System is going to check weather T-code is available or not using TSTC

2) If it is available system is going to check weather T-code is locked or not using SM01.

3) If the T-code is not locked system is going to check weather we t-code is or we maintain the t-code against the authorization object S_TCode (against the field TCD).

4) System is going to check weather we maintain appropriate objects or not authorisation object and also values (or) not.

→ If all these steps are passed, system checks in the ABAP PROGRAM is there any authorization object (or) values are maintained against "AUTHORITY_CHECK" command.

2) Why the authorization object S_Tcode is also called as FIRST LINE OF DEFENSE

A) Because when we add T-code in the menu it is going to store in the authorization object S_Tcode against the field 'TCD'.

3) How the Profile name is generated (in Role after Generating the authorization object)?

A) 'T_' is common for profile name (10 characters) (T_ (2 characters))

Eg:- T_E7552226.

→ 'T_' these two characters are common for each and every profile

→ Third and 4th letters are characters are (eg:- E7) are 1st and last letters of SID (EH7) i.e E7.

(59)

AGR_NUM_2 :- This table shows list of Profile names.

→ for every new role generation the profile name value will be increased by '1'.

→ We can edit profile name but we wont prefer it.

AGR_Tcode :- This shows relation ship between Role & T-code.

USR04 :- Relationship between User & Profile is seen in this table.

4) Why maximum number of profiles assigned to user is 312?

A) → USR04 contains field PROFS (Technical name for User Profile(eng name))

→ length of the field PROFS is 3750.

→ When we generate role profile is generated and length of profile is 12 (which includes before & after space while adding.

→ 2 characters are mandatory '1' is for create, '1' is for Modify.

312 X 12 = 3744

adding 1+1 = 3746.

3750 − 3746 = 4 (As profile is length 16 so it is not possible to add another profile (as it is 4))

→ Number of profiles should not exceed 3746 (max it doesn't exceed).

→ In Real time we won't do any kind of modifications in profile name.

Note: If no T-code is assigned in menu and then if we click on authorization it shows a Template.

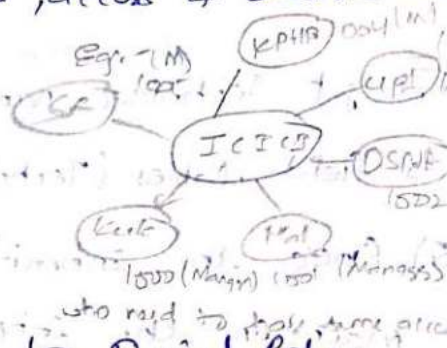
Authorization status:-

1. Standard:- These values are default values in authorization fields
2. Manually:- The authorization object & object field values are given by user Manually.
3. Maintained:- The changed values have been maintained in authorization fields (ie maintain SAP field with user given values). (eg:- ☐ ;→
4. Changed:- The default values of the authorization authorization fields have been changed. (The value provide by SAP is changed as per the requirement (eg:- SAP field value 01, changed to

13/2021 ★★★

Derived Role:- Some job function & responsibilities can perform in different geogr locat

Master Role:- We maintain Master Role with all the information (Org values with * & other values like authorization objects & field values) so that we derive everything from master role to the derived roles (who need to have same permissions, access & restrictions which is not much time consuming.



→ Derived role is nothing but a single role.

→ There will be no access to Transaction Tab in Derived role

→ Except Org values other info will be derived to Derived Roles.

Master Role:-

PFCG → Role [YAM: ICICI : MAN - MAIN] → single role → description

[Master role for Manager] → Menu → Transaction → XK01 → Assign Transaction → Authorizations → change Authorization → save → company code [*] → after assigning values → Generate → save → after creating derived role this [☐☐] will be displayed to generate the info to the derived roles.

→ It inherits to parent and child role.

Derived Role:-

Process of creating and assigning Master Role is as

PFCG → YD_ICICI_MAN → Description [ ] → In Description you'll find Derived role YM:ICICI:MAN:MAIN → Go to Master Role and click on [ ] → This Generates all the Menu, Authorizations to this Derived Role.

Note:
→ Manually we have to create Roles for each and every Manager Role

→ Org values need to be maintained independantly in the derived roles

→ Roles and Users are client dependant.

→ Any changes will be done in Master Role.

AGR_Define :- Relation between Master role and derived role.

SE16N → AGR_Define → Role [ ] → Role → execute
(Role → master, Role → derived)

To get Technical names for the above settings → user parameters

→ field tables (Technical names) is

Q) Once the inheritance is broken in the derived role can we maintain the inheritance?

A) Cannot be regain the inheritance.

Q) Can we maintain inheritance again?

A) No.

Q) Why we use Authorization tab?

A) Simple answer to generate profile.

Note:
→ If we remove T-codes in the Menu in single role in them derived role will be open to maintain it we remove T-codes in menu we that it will be as a single role.

→ In real time we wont break the inheritance mostly.

→ Copy data (tab in single role Authorization). & Generate the derived ( )
act as same → copys to partial derived role
copys to all derived roles.

→ Derived role is nothing but deriving from the existing role. ①

→ Copy data & Generate the derived (👥) roles are same because to avoid maintain values manually. (57)

→ Befor versions EHP5 it is possible that as the above both are different

→ After EHP7 both are same (copy data & Generate (👥)).

Note:- Breaking the inheritance will only happen if the plant closes.

→ BASIS team will send from QAS to PRO & informs to the security consultant.

→ After this we need to inform Roll owners (Role) that it is in 'pro' then after getting approval we need to close the ticket (we should not think that if it is pro the process as ended if the ticket status is closed then its done).

Note:- If one user from the Derived role wants spec. extra access for 1 hour in this scenario we won't create role each & every time (creates only if the user needs for more time (6 months)). We give sap-all (or) lesser role to the user and Remove.

Q) Which table shows profiles for composite Role?

A) PROFILES won't be generated for composite Role so there is no table for this.

Q) What if in one authorization object one field is "Maintained" and other is "changed" what will be the status of the main authorizations?

A) Changed (it always overrides Maintained).

→ "Manually" is least preffered status. (4)

→ "Standard" is most preffered status (1)

→ "Maintained" is the third preffered status (3)

→ "Changed" after standered this is preffered (2).

Q) How to find how many objects are added manually in a role?

A) AGR_1251 - list of fields & values fn in a role

SE16N → AGR_1251 → Object status → "execute"

AGR_1252 → list of org levels and values of a role.

SE16N → AGR_1251 → Role → execute

→ Δ (where by) → This symbol in new versions are had been removed because as it consumes more space (Graphical Image) we can find it in utilities → where used by. (It shows the T-code where has used previously).

'A_' starting with 'A_' is Accounting Authorization Object.

S_User_TCD → This Authorization object helps to restrict the T-codes.

S_User_VAL → This Authorization object helps to restrict the Activity values (can only add prefered values which have been maintained)

2/3/21

Important topics in SAP ECC:

1. CUA 2) Derived Roles 3) Table Security 4) SU22, SU24, SU25.

User Buffer:- Stores temp. files. Whenever any user login's into the system till logout all the transaction codes, roles and everything will be stored into user buffer.

SU56 - Authorization objects, Roles, profiles, values stores in this helps to reset User buffer.

SU56 → Authorization values → (fourth in the top menu bar) → Reset user buffer

Q) Inspite of assigning roles to users, user is going to be complain that T-code is not working?

A) 1. Ask the user to logout and login first. then if it doesn't work.

2. Check wheather user comparision is completed (yes) not.

3. Check weather 312 profiles are exceeded (or) not.
4. Check the validity period of the roles (SU01 → roles tab).
5. If expired roles are there delete all the roles (USR04 → against profile field).
6. Reset Bufkr.

(59)

Q) Which is better Role (or) Profile?

A) Role is better because it has naming convention. (easy to identify eg: ph.no without names).

→ If we want to reset bufkr for different user.

A) SU56 → → click → user [ ] → execute

Q) What are the options when we execute SU56?

A) User name, Instance, System, Date, No. of authorizations, Authorization object, client, Time, profile parameter auth/ new buffering.

Note:- If we reset user buffer, roles will not be deleted, only temp files will be deleted.

Q Reset user buffer for all the users How?

A) RSUSR405 :- To reset user buffer for all the users

***

Table Security :-

→ If any user wants to access the table we assign SE16/SE16N. to user. There is a chance to commit a fraud because table contains information.

→ There are four ways to restrict the tables (1,2 will be done mostly)

1. Restrict the Access against Table Authorization against Groups level (S_Tabu_Dis) → (Authorization object).
2. Restrict the access against Table name level (S_Tabu_Nam).
3. Restrict the access against Table client level (S_Tabu_cli)
4. Restrict the access against Table line (colum) level (S_Tabu_lin).

→ Until 2011 we used S_Tabu_Dis.

→ If any user wants to access any table (USR01) till 2011 we used S_Tabu_Dir.

1) We need to check in which group the table belongs to using the table TDDAT.

2) How many tables are there in particular group using 'TDDAT'.

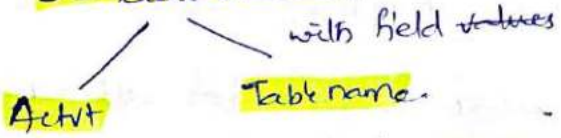
→ We can access all the tables in the group.

Drawback:- If the user needs access to one table but when we assign this group there is a chance to commit a fraud because there are more tables in the group.

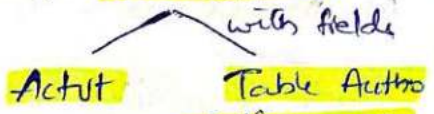
→ To overcome this SAP recommended to create our own customized each & every table by table group (eg:- 300 tables → 300 groups).

SE54 → To create customized user table and assign it to the user (if we have more than 2 tables in the group).

→ After ~~2001~~ 2011 SAP introduced S_Tabu_Nam.



Note:- To work in S_Tabu_Nam we have to deactivate S_Tabu_Dis.



→ DICBERCLS :- Technical Name for Table Authorization group.

TDDAT :- Stores Maintenance Areas for ~~dat~~ Tables data.

Practical of Table Security:-

(1) S_Tabu_Dis:- Eg:- User wants to access the table agr_agrs.

a) check wheather in which group the table belongs to using table "TDDAT."

SE16n → TDDAT → Table name AGR_AGRS → execute. (we find table group like 'BUS')

b) check wheather how many tables are there in group using "TDDAT".

SE16n → TDDAT → Authorization BUS → execute. (Its bets best to use SE16 table for practice)

Note:- Authorization Groups starting with 'S' are standard group.

→ Create Role first T-code SE16n & create group and assign to user. (6) (1)

PFCG → Create role → Authorization object → Manually [S_Tab_Dis] → Activ [3]
→ Table Authorization Group [SC] → menu → Transaction [SE16] → Assign authorization.

→ Creating customizing Table Group and assign table (eg: USR02) using SE54.

SE54 → Authorization Groups ⊙ → create/change → new entries → [Zgrp]
→ Description [ ] → execute → accept profile [✓] → Assign Auth Grp ⊖ →
create/change → Table name [ ] → ⊖ Authgrp [Zgrp] → save

Note:- Any customization group (eg: Zgrp) name starts with 'Z' (or) 'Y' (it won't accept more than 4 letters).

Assigning Customizing Group with table to User:-

PFCG → create role → Tab Authorization Group [ZGRP]

Note:- &NC& → Tables not assigned to any group are stored in this.

(2) S_Tabu_Num:- Firstly we need to deactivate (☐) S_Tabu_Dis to access this.

→ Same as creating role Manually add this Authorization Object (S_Tabu_Num).

Activt [03], Table name [USR01, USR02, USR03 —] → can add what are required for user → Generate.

(3) S_Tabu_cli:- To restrict the table for client level.

we give particular client in the field.

(4) S_Tabu_lin:- To disable the field i.e for particular column. (eg:- aadhar column is of no use for US people).

SU21:- for Security Consultant if there is no access for SE16/SE16N at that time if this SU21 is used to know what are fields are there and what are the permitted activities are there in the particular Authorization object.

② If ABAPERS want to create customized object classes & also to Create authorization objects they use this SU21 T-code. (67)

SU21 → find S:tabu-dis → double click on the A.O → execute → you'll find the values & fields → scroll down → Permitted activities → click.

TACTZ :- If we don't have access for SU21 we use this. (stores Pakash sir data) valid Activities for each authorization object.

* If ABAPER joins in a company what he needs to have.

A) 'User Id' and pass' is required first.

SE38 → To create Program

SE38 → source code → Access key [ ] of 20 digits.

→ ABAPER needs Development key to create a program. (it is one time generation)

→ Development key can be created using the following ~~website~~ Market place.

Support.sap.com → Market place (site).

↓

asks user Id & pswd.

↓

'S' followed by '10' digits → (will be security Consultants Id).

↓ → Generate key ↑

asks 3 options.

↓

asks userId of ABAPER who needs the 20 digit key.

DevAccess :- Stores the Access key of users (20 digits) and to know how many developers are there in the system.

→ ABAPER can work from two objects.

1. Standard object :- Need to have user id, developer key, Object key (20 digits)
2. Customized object :- No keys required except development key because he is building from scratch

Note:
→ Object key needs to be generated every time (i.e for each new program).
→ Apart from all these ABAPER needs to have access to the Authorization objects S_develop, S_program.

S_develop:- This Authorization object is assigned to user to develop a program.

S_program:- This Authorization object is assigned to user to execute a program.

Adiraccess:- All the object keys are stored.

Q) Where do you generate development key?

A) from Market place.

Q) Will you show how to login into market place?

A) Shared to team (not remembered).

Note:- When ABAPER is modifying a standard object he needs object key.

TSTCP :- Substitute T-codes stores in this table.

Note:- We need to lock substitute Tcodes (because if a user doesn't have access to SU01 but has access to the substitute T-code of SU01 which ~~are~~ is same.

SE16N → TSTCP → parameter *SU* → execute

Q) Why is S_Tabu_Dis is disadvantage?

A) Because every time Role & Group has to transported separately from Development to QAS & PRO. ~~every~~ for each one which is to more process.

S_RFC → This A.O helps to execute RFC's

S_RFC_ADM → This A.O helps for admin users to create, Modify.

* Difference b/w SU01 & RSUSR406?

A) SU01 maintains authorization objects (reflects to particular object).

RSUSR406 is to generate Sap-all (reflects to all the clients in the system).

(we mostly use this when abapers creates new obj's or ~~obj~~ message generate it to reflect).

3/3/21

~~SE91~~ SE93 :- To create our own customized T-codes.

(64)

4/3/21

SU20 :- To maintain Authorization fields.

SUPC :- To generate Mass Profiles.

SUPC → execute → click on ▨ (to select all) → Generate.

~~Venkanth sir class~~ (In real time if we are into support this is the task we do).

SU53 :- To evaluate last failed authorization check (what is missing to user.

→ If some user doesn't access the T-code and if he informs Security consultant we need to ask for SU53 screen shot.

→ ~~If~~ ~~the~~ If the user sends the screen shot we need to check the ~~the~~ wheather the ~~User name~~, ~~Screen shot~~ (taken ~~in the~~ ⊖ Username (check that the same user took the screen shot (or) not) and system (eg: ⊖ II 7), (i.e took in the same instance of user), in which client, and we can see ~~in~~ which T-code user is executed.

→ Go to SUIM → Roles → Roles by complex selection criteria → object S_Tcode → value SU01 → execute (i.e we have to check wheather that t-code is assigned to that particular user (or) not).

① → for practice create a user & assign a role having t-code (SU53) to username SU53_user → create → assign a role with (SU53 & SU01) T-codes in it with no field values → Login to SU53_user → SU01 → Try to create new users → you are not authorized → In SU53 (from same session) → Take a screenshot.

② Now, after getting screen shot the next step is to go to SUIM and check the appropriate roles suitable to the user.

SUIM → Roles → Roles by complex selection Criteria → In selection according to authorization Values → object 1 S_Tcode → Value SU01 → execute.

③ Now we have to select appropriate roles suitable to user by ~~his~~ depending on org levels (location, plant) etc.

④ After finding the appropriate roles we need to send the roles (2,3) ① to Role owner to pick the appropriate role which is to be assigned to user (if any role is suitable we need to ask for approval (mail for Role owner). If the roles are not suitable in SUIM ask RoleOwner whether to create a new role if yes ask for mail approval. (5)

Note: We only search for a suitable roles we won't modify/create new roles.

→ There will be existing roles we have to check & which roles are suitable to user (using SUIM).

Note:- Object level will always be the correct one to check T-codes (S_TCode) because Menu (in PFCG role) T-codes and authorization T-codes (manually added T-codes) all are going to store in object level.

TRACE :- Failed authorization check T-code. (It shows all the failed authorization checks of user.

Drawback of SU53 :- Using SU53 we have to remotely login to users account and rectify the issues but using TRACE we can login to any instance with our UId tps (no other we have to know the user Id of the user who cannot access the T-code so that we can search).

→ SU53 only checks last failed authorization check. Using this we check all failed authorization checks.

STO1 :- This T-code helps to enable Trace,

① firstly we have to check in which instance he is logged in using ALO8.

ALO8 → check in which instance he is logged in

② check the instance in which the user is logged on. using SM51

SM51 → click on select the instance → click on Remote logon → STO1 → ☑ Authorization check ◉ All → General filters → In popup → Trace for user only [SU53_user1] → click on [✓] → Save settings → Trace on → execute the T-codes in user SU53_user1 (issue T-code), → Trace off → Analysis → User name [ ] → From & To if needed → Execute.

Note: After Analysis you'll find RC values "Return Code". There are 3 'RC' values they are 0, 4 & 12

→ We only check 3 'RC' values (Security Consultants). (6)

RC = 0 → Successful (eg: Tcode exists).

RC = 4 → Object is there but value in the field is missing (eg: Activity (01,02)).

RC = 12 → Object itself is missing.

Q) If T-code is not there what is the RC value?

A) RC = 4 because in object value (T-code) is missing).

Q) Why Trace is not working?

A) We have to check in which instance we have logged in (i.e user instance)

Stauthtrace:- Same as ST01 in this we can skip two steps ALOG & SM51.

→ We can check Trace for multiple users using Stauthtrace T-code.

→ It is system wise trace.

Stauthtrace → Trace for user only [SU53_user] → ⊙ evaluate.

→ It is user friendly.

→ Note: If we don't want 'RC=0' in result click on "Trace for error only ☑.

→ We need to off the trace after the work has done because sys sometimes systems can crash as it records logs of the user if Trace on.

→ And if someone use trace the other cannot access trace. So that after the work has done we need to off Trace.

USR07:- List of last failed authorization checks.

Note:- After EHP6 SU53 records 100 last failed authorization checks but we won't go for this we use "Trace".

Difference between SU53 & SU56:- In SU56 if the data (Tcode, or anything) is not available that will be displayed in SU53.

Q) What if we found 0 records when Trace is on?

A) Some times time zone is different (This will be set by BASIS people)

Q) What if we find '0' roles for the user? (In SU53 related roles).

(64)

A) We contact POC.

5/3/21 SU53 (extra topic extended by Rajesh).

→ We have two authorization issues which we get regularly?

1. User need to access a T-code.
2. Has access the T-code not able to carry out any authorization.
   → send the ss of screen shot of SU53 (Ask the user)
   → SU53 displays last missing authorization previously upto ECC6 after ECC6 it displays 100 last missing authorizations. Based on this we do the steps.

Using SUIM → Roles → Role by complex selection criteria → Authorization object S_USER_GRP → Activt 01 → execute. (as the user is missing SU01 value of 01).

→ If you the result get 264 (eg) roles by using role naming convention you found 48 suitable roles as. And then we send them to the roll owner if he says to assign some particular role (eg: y/c) we assign that.

Note:- Most of the times we resolve the issues using SU53.

→ If sometimes if you are not able to solve issues by SU53 we go for trace.

→ To switch on the Trace we have 2 T-codes.

1. ST01 & 2) Stauthtrace.

→ We have to make sure before clicking on analysis we need to remove the time & date against the analysis screen.

→ In ST01 if the user is in same system (800) then we trace in (810) we login to 800 and do the tracing.

→ STAUTHTRACE 800, 810, 811 } from the same system we login to other client and on the tracing.

V.V.Imp ★★★

SU22, SU24, SU25 :-

SU22 :- When we install SAP all the authorization default values are stored in the tables USOBX, USOBT (eg: some auth obj are pulled from some where). ~~This is stored~~

USOBX :- This table contains object class, authorization objects and fields

USOBT :- This table contains values (that some values are given by SAP)is better value

→ Note :- As SU22 is standard so that we won't modify anything in this we use SU24.

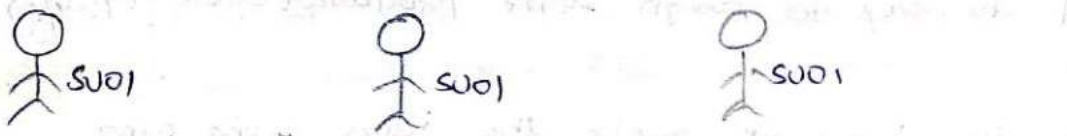
→ ~~It~~ To copy data from SU22 to SU24 we will use the T-code SU25.

→ This is only one time activity (at the time of implementation).

→ Some of the authorization objects will be pulled from ~~SU~~ SU24 (in Roles Authorization).

→ We don't do any modifications for SU22.

→ We modify SU24, But when we modify SU24?



Auth obj S_user_grp	Auth obj S_user_grp	Auth obj S_user_grp
Actvt - 01, 03.	Actvt - 01, 03	Actvt - 01, 03
class - Ind, Aus	class - Ind, Aus	class - Ind, Aus

→ For example if the Actvt value 03 need to maintained for so many field values then its ~~hectic~~ time taking to provide to each and every field so that we maintain predefined by using SU24.

→ What are all common values are there we will maintain those in ~~SU~~ SU24 [like fields, values, Auth objects).

→ When we add T-code in Menu Tab some of the authorization objects are pulled from ~~SU~~ SU24.

Check Proposals: There are three types of check proposals (why only few Auth objects & values are pulled from SU21 because of these check propo -sals. (69)

1. **Check Yes** :- Whenever we add any T-code in menu some of the authorization objects are pulled from SU24 because of check-yes (System is going to check against the Auth object which are 'yes' and pulls).
2. **Check No** :- 'No' values will be pulled to the Authorization screen.
3. **Check Do not check** :- This is dangerous for HR & BASIS (neither check nor pull it).

Practical:-

→ firstly we create a role.

PFCG → Role name [ ] → menu → Transaction [SU01] → Authorization → change authorization → Generate → save. S_USER_GRP → Activt = [03, 05] → default values generated.
→ Generate → save

→ Now we execute SU24 and change the values 03, 05 to 01, 05:-

SU24 → Type of application (Tab) [Transaction] → T. code [SU01] → execute → Display transaction SU01 → Display change → Double click on S_USER_GRP → change values → Activt - [01,05] → save. → work bench request (Client independent).

→ Once checks are performed changes will not reflect immediatly: (in current role it will not reflect). Create new role and check autho -rization objects the values 01, 05 are pulled as we changed in SU24.
In real time Role owner gives values accordingly as per requirement.

→ The modifications will be reflected to new roles only.

→ If you want to apply new modification to old roles there are three expert mode options (in Authorization Tab) PFCG.

PFCG → Authorization Tab → Expert Mode for Profile Generation

1. Delete & Recreate Profiles & authorizations.
2. Edit old Status
3. Read old status and merge with new data.

1. Ddete and Recrate Porofiles and authorizations:- What ever the values and authorization objects assigned to roles those will be deleted and creates new role and pull the data from SU24.

2. Edit old Status:- Same no change.

3. Read old Status and merge with new data:- It Reads old data (this don't get be deleted) and the modifications will be added to the authorization objects.

Note:- Mainly we go for third option as one SAP recommended.

SU25:- This T-code helps to copy the data from SU22 to SU24. If it is a fresh system then we have to copy this is only one time job.

SU24:- Same as SU22 but USOBT_C table will be empty.

USOBX_C (C-indicates copy/change) :- Contains objects class, Authorization objects, & fields

USOBT_C :- Values (but this table is empty).

Q) What if client asks the Authorization objects for SE16N.

A) SU24 → Type of Application [Transaction] → Transaction code [SE16N] → execute

→ Using SU24 adding Authorization object?

SU24 → SE16N → click on change/Diplay → Object → Object → Add Authorization object → Authorization obj [ ] → ☑.

→ ~~After~~ Transporting Concept:-

→ After modifications we have to move to QAS & to PRO.

→ Only when you move transport it to QAS and to Dev then it will be consistent

→ After the changes has done we need to transport it by work bench request (role) (Description, user).

need to be given provided.

Auth. objects:

S_Transpri,

There are two types of Requests

1. Work Bench Request and (Client Independant) Eg:- OSR40, Logical system, SU24 changes, SALE, Authorization Groups, SE54.
2. Customizing Request (client dependant)

   Eg: Roles.

Note:- Users creation don't have request because they are client dependant and as they can be created in the required system (DEV, QAS, PRO).

Derived Role Transporting:-

PFCG → view → Inheritence → select the Master role → dropdown of master role → you we can find child role → select either master role or child role (as child role inherits the parent role) → click on Transport (truck) → ☑ Generate profiles of single Roles → execute → Customizing Request → Create Request → short Description ☐ → User ☐ → save → ☑ (in Prompt for Customizing request).

Mass Transport:-

SE16n → Tablname ~~Arg~~ Agr_Define → select child roles → copy (as it is easy if there are many child roles).

PFCG → utilities → Mass transport → ☑ Generated profiles of single roles → execute → Customizing Request → Create Request → short Description ☐ → user ☐ → save → ☑ (in prompt for customizing request).

Releasing a Request:-

SE01:- This T-code helps to create a Request.

SE01 → copy the transport request (~~in~~ customizing, work bench) eg: E11K901502 → user ☐ → ⊙ customizing Request → ☑ Work bench Request → ☐ (create) → ⊙ customizing / work bench request → short description ☐ → user ☐ → save

(or)

SE01 → Display → ☐ create → customizing ⊙ / work bench ⊙ → save

S_Transport:- Need to have this Authorization object to transport the request with Actvt value 43 (Release)

Note:- After creating the request we need to mail to BASIS team that move it to QAS.

→ If it is customizing BASIS team will move it to other clients.

→ If it is workbench BASIS team will move it to QAS.

Q) How can you transport derived roles without PFCG access?

A) Report: PFCG-mass-transport (if there is no access to T-code PFCG)

we use this Report to transport Roles.

6/3/2021

USR03 :- This table contains Name & Address of all users.

SU10 Drawback:- 1) Passwords need to be copied and send to the appropriate users., so organizations maintained their common password to get this we use ECCAT script.

How to remember data :- 1) WIN - Workbench Independant.
2) CD - Customize dependant.

Transport files :- Two files

→ Data files :- Actual data (whether we are missing Roles, programs).

→ Co-Data :- Attributes of the transport request who created the T.R in which client the Transport request is created.

Options while we transport a Role:-

1. Generated Profiles of Single Roles:- Profiles in the role need to be moved or not.
2. Personalization Data:- Tab in Roles, that data need to be moved or not.
3. Direct User Assignment:- Same role in Dev (user) is assigned to QAS to that user (don't use this).

→ When we accept the transport request that is Co-data and we get get another transport request that is co-data file.

SE01, SE09, SE10 → These are T-codes are used to transport request.

There are two types of transport status:- (Modifiable, Released):-

→ As far as the transport request is not released we can do 'n' number of modifications (modifiable) with the help of Transport request number.

Q) What are the tables that are moved while we transport role? ①

A) AGR_TIMEB } - Time when the Transport Request has been released.
SPERS_OBJ }

(73)

→ If we want to release Transport Request we need to release data file request (Click on Touch).

→ If we want to release Transport Request we need to release Co-file later.

Released:- We cannot do any modifications after the Transport Request is released.

E070 :- Status of This ~~table~~ table shows the status of Transport Request (i.e Released / Modifiable).

E071:- Actual data (objects with in Transport Request) eg:- Roles, Programs.

'D' - Modifiable (Status of Transport Request).

'W' - Customized Request:

→ Same Request number need to be there in three systems i.e Dev, QA, and PRD.

→ Until and unless Transport Request is Released we can add 'n' number of roles in the same request instead of creating new requests as per the requirement.

Sritanth sir class.

Q) What are check proposals and check indicators?

A) Check proposals:- Check Yes, check No, check do not check.

Check indicators:- RC=0, RC=4, RC=12.

Note: when ever we schedule Back ground job we use system user type.

*** Background job (Handled by Basis Team):- PFUD:- Which will help you to do mass comparision to users (in Role we do only one user comparision)

→ GRC tool will not do mass user comparision, But it assigns multiple roles to users.

→ To avoid this, concept Background jobs concept has came we can set time manually by Background jobs.

PFUD → Role | Test SU53 | → execute

→ User comparision will be in Red first, after doing the job of by PFUD it can be the status can be green.

→ To avoid PFUD.

PFCG - time - Dependenty → Report This Reports helps to avoid PFUD. when there is no access to PFUD we use this Report. It is client dependant. It does user profile comparision to user. Eg:- If user expires by using this we it to delete it).

SA38 → PFCG - time - Dependenty → execute.

→ This has to trigger at particular time (Background job). Because for example user can access after the expiration also if there are new users user comparision will be done.

PRGN_COMPRESS_TIMES:- Report to delete to expired roles entries (in previous profile will be deleted but role will be remained so that using this we can delete roles (which are expired) same role dw and also duplicate rdes will be deleted.

Note:- By this two Reports, Reports will not be deleted only user comparision and expiring roles and duplicate roles will be deleted.

SM36 :- Helps to schedule a background job.

SM37 :- To monitor a background job (SM37 → execute).

SMX :- Defaulty this T-code is assigned to users. This helps to check for the user by himself (Background job).

To Remember Background jobs:-(Tip)

S - Schedule
R - Released
R - Ready
A - Active
F - finish
C - Cancelled

} statuses available for background jobs.

Job classes found in Background jobs:-

A - High
B - Medium
C - Low.

Note:- BASIS people will set file size while Traving. and also mentions data how as many

Practical of Background job:-

SM36 → Jobname [SEC_USER_COMP_Dai_N] (naming convention need to be maintained (to identify security / Basis)) → Job class [A] (high) → step →

Save → user [ ] → we won't provide user id here as we trigger this job thru using some id's (Batch id's, system id's & Generic id's). → ABAP PROGRAM (click) → Name [PFCG_time_Dependancy] → (Clown) check (click on) → save → Go back → start condition (click on) → As of now selecting Immediate → Periodic ☑ (as we click this it asks for more info about hourly, monthly → click on Check → save.

* Until and unless you click on save it will be active.

SMX:- Directly shows the status.

Deleting Roles to user (expired roles):-

SA38 → [PFCG_time_Dependancy] Job name → execute → user [Betty] → ☑ Delete expired assignments.

* option ☑ Simulation Run :- shows that.. user has expired role entries and duplicate roles

* If naming convention hasn't given properly for Background job then its hectic to check ~~every time~~ in lots of data every time so ~~we have~~ that the tables are given for this

Eg:- SEC_USER_comp_Dai_L (Security_user_comparision_daily_low).

TBTCP:- This table shows for particular program name (eg: PFCG_time_dependancy) what background job is scheduled will be displayed

TBTCO:- This table shows when the Background job is scheduled, time and status of (Background jobs).

Authorization objects:- To schedule Background jobs user need to have these Authorization objects.

S_BTCH_ADM → full Access to user (Admin) → field (BTCADMIN) ☐.

S_BTCH_NAM → To check for particular user → fields (BTCUNAM - ☐

S_BTCH_JOB → Apart from Scheduling other jobs will be accessed to user.
fields ← Job group ☐
Job action ☐.

SUIM Assignments:-

1. Find the list of T-codes executable for DDIC ?
2. Find the list of T-codes executable for role SAP_AUDITOR_ADMIN?
3. Find the list of roles which has T-code OB52?
4. find the list of users having access to profile SAP_all?
5. Find the list of users who belong to the group SUPER?
6. Find the list of roles having the authorization object S_RZL_ADM with ACTVT 01.
7. find the list of users who were assigned SAP_ALL in the last 6 months.
8. find the list of users deleted in the last 1 month.
9. Find the list of users created in the last 1 week.
10. Find the list of dialog users in the system.
11. Please find the list of users who are having access to the T-code (SU01).

Role Administration Assignments:

1. Please find which authorization objects are pulled when the T-code MM01 is added into menu of the role?

A) PFCG → create a role → add Tcode MM01 → Authorization Tab → MM_G → M_MATE_BUK, M_MATE_LAN, M_MATE_MAN, M_MATE_MAR, MAT, MEX, MZP, NEU, STA, VKO, WER, WRK.

2. After adding t-code MM01, for which authorization objects values are not completely maintained?

A) M_MATE_MAR, M_MATE_MAT, M_MATE_STA, M_MATE_WGR.

3. Please main-tain * values for the authorization objects M_MATE_MAN and M_MATE_MAR and note the authorization status of the authorization objects?

A) M_MATE_MAN → changed, M_MATE_MAR → changed.

4. What is the status of your authorization Profile?

A) changed.

5) Please find which authorization objects are pulled when the T-code XK05 is added into menu of the role?

A) F_LFA1_AEN, APP, BEK, BUK, GEN, GRP.

6) Please find which org. levels are pulled when the T-code ME21N is added into menu of the role?

A) Purchase group, purchase organization, Plant

Table Security:-

1. Find the list of tables which are part of the authorization group SS?

A) SE16N → TDDAT → Authorization [S1] → execute → (2,260)

2) What are the fields available in S_TABU_DIS?

A) Activity [ ], Trd Table Authorization Group. [ ]

3) Find the list of Authorization groups starting with the letter S?

A) SE16N → TDDAT → Authorization → S* → execute → (7,538).

4) Create a Authorization group Z251, maintain table agr_1251 into Z251, find the dist of the tables in the auth. group Z251 (1 agr_1251)?

A) SU54 → ⓐ Authorization Groups → create/change → New entries → [Z251] → save → Go back → Assign authorization groups → create/change → Table [agr_1251] → Assign group [Z251] → save → ~~PFCG~~ → SE16N → TDDAT → Authorization [Z251] → execute → (1).

Client Administration:-

1. Find the no. of clients available in the system.

A) SCC4 → Execute → F5 / SE16N → TOOO Table to be searched → execute (15).

2. Find the client Role?

A) SCC4 → New entries → double click on client which to modify → client Role

Customizing for SOT.

3. Confirm if the global states is set to modifiable or not modifiable?

A) SE06 → system change option → can be set to modifiable (in drop down)

4) How do you open and close the client?

A) Client open: SCC4 → click on create/change → double click on client (to be changed) → customizing

→ No changes allowed, No changes to repository and cross client customizing allowed.

SUIM Assignment Answers:

(141) addl

1A) SUIM → Transactions → Executable Transactions / Executable for User → User id

2A) SUIM → Transactions → Executable for Role → Role SAP_AUDITOR.NMM → execute (25)

3A) SUIM → Roles → Roles by complex selection criteria → Transaction code OB52 → execute (471)

4A) SUIM → users → users by complex selection criteria → Profile name sap_all → execute (419)

5A) SE16N → USGRP_USER → user group SUPER → execute (162) / SUIM → users → UBESC → User group SUPER (165) → execute

6A) SUIM → Roles → RBESC → Authorization object S_RZL_ADM → Activ 01 → execute (54).

Enter

7A) SUIM → Change documents → for users → Set from date to to date → Roles/Profiles

profiles ☑ → profile name sap_all → execute → (588).

8A) SUIM → change documents → for users → set date → users deleted ☑ → execute (940).

9A) SUIM → change documents → for users → set date for week → user created ☑ → execute → (304)

10A) SA38 → RSUSR200 → ☑ Dialog user → execute → (3,081)

11A) SUIM → users → UBESC → Transaction code SU01 → execute → (3,012).

10A) SUIM → users → UBESC → execute filters at users types.

7/3/21 **Note:-**

Deleting duplicate roles which are assigned to user is done by choosing the 1st date (i.e the role ~~created~~ assigned date of 1st role) and the last date (i.e the validity end date of the other role) and delete's the duplicate role

(19)

06-01-2020 to 31-03-2021
26-08-2020 to 30-12-2023.

Chooses 06-01-2020 & 30-12-2023.

Q) Inside the Authorizations what are the Traffic signals?

A) - Org values are not assigned, field values, Authorization objects are not assigned then it is (Red.)

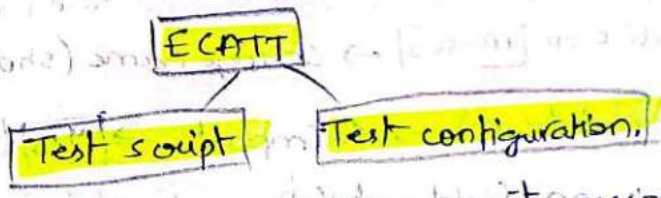
Note:- In Background job after clicking on Periodic values start condition these periodic values will be there.

Hourly, Daily, Weekly, Monthly, Other Period.

***

Ecatt Scripting:- Scripting for SU10:-

→ We download the script once & perform all the time.



Test Script:- If mistake happens it records and need to start the script from scratch. we use common organization pswd here.

Test Configuration:- We download the file and we can use the file many times once you configure and we open it into txt. file excel sheet too and use many times to create mass users.

* In test script & SU01 we need to maintain user name, Last name, pswd & conform password (it happen in the middle of ~~este~~ ecatt process)

→ After ~~fetch~~ SU01 (as we fill details) and sending to Test configuration we need to change the field names.

SECATT:- This T-code helps to perform Test script and Test configuration and also uploading file job.

ECATT - Extended Computer Aided Test Tool.

Practical of Test Script:- Befor doing ECATT need to set ECATT settings. SCC4 → double click on client → ecatt setting (Allowed).

SECATT → ⊙ Test Script [Y_users_creation] → Create → Title [mass user creation] Application component [BC-SC-C-USR-ADM] → (This will be get by click drop down, select BC(4) → BC-SEC ⊕ → BC-SEC-USR ⊕ → BC-SC-C-USR-ADM) → save → Create Object Directory Entry → Package → click on [local object] (it selects default package $tmp) → click on Pattern → Group [user interface control / UI control.] → (in dropdown select this) → Command [TCD (Record)] → (In dropdown select) → Transaction [SU01] → After clicking on continue → Interface [SU01_1] will be automatically generated. → Click on [✓] → (Takes to SU01 screen) → user [mass12] → lastname [mass] → Logon data → New password [12345678] → Repeat pswd [12345678] → save → Click on back button → Goes back to secatt screen → Asks Do you want to transfer data → click on [Yes] → Click on [TCD(SU01, SU01_1)] → Asks do you want to save data → click on [Yes] → click on (SU01_1) → click on Dynpro (dropdown) → [1] (dropdown) → double click on field → double click on [MASS12] → again double click on [Mass12] → change name (should start with 'Y' → [Ymass12] → click on ⇦ (Back) → ⊙ Import → [Yes] (click on) [2] dropdown → double click on field. → Invalid → double click on lastname [mass] → Again double click on [Mass] → change to [Ymass] → Click on ⇦ Back → ⊙ Import → [Yes] → [3] dropdown → double click on field → In value double click on password (New password 12345678 & Repeat password 12345678) → change both values by one by one by double clicking on it → click on ⇦ Back → ⊙ Import → Yes → save → (After this we perform Text configuration).

Test configuration Practical:-

Go back after saving Test script → ⊙ Test configuration [Y_user_creation] → Create → Title [mass user creation] → Application component [BC-SC-C-USR_ADM] → save → click on local object → click on [Configuration] Tab → Test script [Y_user_creation] → save → download variants (Click on bounds in Top) →

SAP GUI SECURITY → click on [Allow] (Asks where to save the sheet (location)).

→ Save as type (Text files (.Txt)) → click on save → ~~Download variant~~ data (pops up) → ~~click on Yes~~ → ~~SAP GUI SECURITY~~ → ~~click on [Allow]~~ → (81) ~~variants will be downloaded in the selected file location.~~

* ~~Note: After downloading the file right click on file to convert the word format sheet to Excel format~~

→ Utilities → settings → Ecatt → click on [External] Tab → select the path in Ecatt object, same variant and Dynpro → continue → click on [] → (Download) button → save as .txt file → save. (file will be downloaded to selected path.

Q) What is the file format when you download in ECATT?

A) .txt file.

Creating Multiple users using Ecatt:-

→ Firstly we need to open the downloaded word Note pad format file to Excel format to do that

Right click on file → open with → choose another app (if you don't find Excel) → and if we don't find → click on look for another app on this PC → All files

→ After converting to Excel sheet format.

* We should not modify first three Rows:-

→ Below variant column list, = numbers (1,2,3,4,5)

→ Below YMASS12 ~~YSHRA~~ Create enter username (mass) with how many you want to create.

→ Below YMASS ~~YETTOU~~ column enter last names of users

→ Below pswd's columns copy paste the password dont include (#).

Note: After filling all the details save the Excel file in the form of Tab (Delimited) Text format.

Uploading the file in SECATT:-

SECATT → ⊙ Test configuration [Y_USER_CREATION] → click on change (button) → variants (click on) → In External file ⊙ → select path of the file → save → popup → click on [Yes] → execute → execute.

Note: We can delete ecatt script which is created by us by selecting the row (side the ecatt screen) and click on (delete row).

SU24 - Auto - Repair:- This Authorization object helps to Automatic Repair of incorrect Authorization Default values.

Note: Org levels maintained in top reflects to all Authorization objects but if maintained in field reflects to particular Authorization object.

Q) While troubleshooting what is the Best RC values.

A) RC = 4 & 12 (because if '0' we cannot know what is the issue is)

Note:- Co file (copy file) has user details who has transported the request.

~~E070~~
~~E070create~~: This ~~table shows~~ created Requests

E070create:- This table shows created Requests of Transport Requests. (no values found when the request is released.

SE03:- This T-code helps to change comment (which we have previously given) in (Transport) | SE09 → we can change short description.

~~***~~ srikanth sir

SE09 → workbench request → double click on request → properties

Merging Tables:- In real time if client asks the data and if that consists in two tables its hard to and time taking task to pull out the data from two tables. So that SAP has recommended this concept of Merging tables if there is **one common factor** which is **same** in **two tables** then only the **merging** of two tables is possible.

SQVI:- This T-code helps to merge two tables.

SQVI → Quick view [Sec_user] (any name) → click on create → Title [USR21 & ADR6 merging] → Data Source [Table join] → Founds in drop down → ⊙ Basic mode → Click on ☑ → (Insert table) click on → Table [ADR6] → Again click on → Table [USR21] → Goback → Select the fields (columns) you want as per the requirement → save → execute.

* After this you can export the table and download the file and make send the sheet as per the requirement. (83)

SAP came up with other concept to avoid SQVI :-

SUIM → user → User Address by Address data (same info can be pulled from this).

Note: We can schedule this as Background job also (SQVI (program → execute → Background (job)).

8/3/21 Srikanth sir

Agr - 1016 :- This table displays how many profiles are created for a role.
→ How many profiles are available with role (when exceeds the limit (150) Auth. obj it creats new profile).
→ In 1 profile we can create 150 objects (Auth objects).

Agr - Prof :- This table shows current profile available with a role.

~~USR41~~ USR41 :- In which instance user is logged in (when there is no access for SM04 & AL08)

Note: Some times very rarely if anything doesn't work for user using user buffer and all (~~login~~ & logout & login) if it won't work.
→ In this case we create new user (need to get approval)
→ or Remove the role & assign again.

Note: In SU01 top in User tab (Rename has been disabled).

* ~~If~~ Need to give Sap_all to user but only in display mode:
→ for profile we cannot mention start date & end date so that for role we can maintain start date & end date.

→ We need to convert sap_all (profile) into Role by giving Activt 03 (01)

PFCG → Role Y: SAP_ALL_DIS → single → Don't give anything in menu → Authorizations → change authorizations → (we can select it from Template) it doesn't find → On Top (Edit) → Insert All authorizations → from profile → maintain Activt 03 for all the Auth. objects which have been generated → until, unless as per company requirement if we don't do changes we should not Generate ⊘ → we only save.

→ Its hectic to give Activt 03 of anything for all the Authorization objects which have been generated. So to overcome this SAP came up with the new T-code.

PFCGMASSVAL :- Directly we can maintain 03 for all Authorization fields (any thing not only 03) using this T-code.

(not maintains as per practice)

PFCGMASSVAL → we can give roles by searching (⊙ simulation (It checks wheather it is applicable or not virtually) → execution with previous simulation → Type of field change (we select appropriate option) → After selecting → click on change Replace if field is empty we ADD → Authorization S_PTABU_DIS → we can maintain particular Auth. obj and value for that

→ Note: In real time we won't or select simulation (checks compatability) & execution with previous simulation, instead we select Direct Execute

Q) How can we execute Report as T-code in command space?

A) In PFCG menu tab we can add Report (Transation drop down) so that the report which is added can execute directly. if we there is no SA38 access.

Note: In CUA parent system we can lock users Globally by clicking lock/unlock in all child systems.

Q) How to identify which role is deleted?

A) By using role naming convention (the role we create) we need to identify which role has been deleted (derived / master).

Q) What is Golden Role?

A) Master Role can be considered as Golden Role

Q) The tables starts with "USH" are refers to what?

A) These are shadow tables for "USR" tables.

Q) How do we get a password change (where to find) for Sap*?

A) from USR02.

Note:- If in Authorization field value the value is "$BUKRS" so if we maintain the org value as "1000" it replaces in authorization field values as $BUKRS. → replaces. = 1000.

Rakesh sir's class

P2P → Procure to Pay (Incoming)

O2C → Order to Cash (out going

R2R → Record to Recruit.

FK01, XK01 → # These T-codes helps to create vendors.

refers to vendor from finance point of view.

refers to purchasing point of view.

9/3/21: Rakesh Sir

S_RZL_ADM :- To maintain RZ10 & RZ11 (parameters).

S_GUI :- This Auth.obj helps to upload and download (Tables)

Actvt: 60 → Export

Actvt: 61 → Import.

Agr_hier :- Table for menu tab.

Note: To create own requests objects we don't need developers key & object key.

How can you change a description of a request?:- → previously given short description

SM30 → USR40 → workbench request → save (illegal password : 404) → if we want to change description.

SE09 / SE10 → select work bench ☑ → ticket → Properties → change / Display → change the text & save.

Note: These changes can be done before releasing the Request. (46)

→ We can change Request owner key.

SE01 / SE10 → change owner (menu) → save

Transport Tables:-

E070, E071, E070CREATE, E070T.

Market Place:- If we want to create keys logon → 10 digits [S002 05 06535] → pswd [ ] → logon → select Request keys

Creating a Developer key & object key:-

SE38 → T-code helps to develop a program (custom program).

→ If the user asks us to create a developer key we use

↳ we use the site support.sap.com (If it doesn't work) use developer key in sap (search in google) / launchpad.support.sap.com.

→ search → Launch the SCCR → Developer key → Register → User Id [sdjae] → Installation number. After this 20 character developer key is generated.

object key in SAP:-

Object key in SAP (search in google) → launch the scr application → object key → Register → objects → program Id [RSTR] → Type [PROG] → after this 20 character object is generated.

Mandatory fields while creating a object key:-

1. Basic Release
2. Program Id
3. Type
4. Object Name.

DevAccess:- Developer keys are stored in this table.

AdirAccess:- Object keys are stored in this table.

T-codes, Tables, Reports and Authorization objects Topic wise:

***

Background Jobs:- (Pg:-73-75)

PFUD:- T-code helps to do mass comparision to user.

SM36:- To schedule background job.

SM37:- Monitor a background job., SMX:- Helps user to check the states of background job (himself).

PFCG_time_Dependency:- Report helps to do mass user comparision (when there is no access to PFUD).

PRGN_COMPRESS_TIMES:- Report helps to delete expired jobs to users.

TBTCP:- Table shows what background job is scheduled for particular program name.

TBTCO:- Table shows when the background job is scheduled (time & states).

Authorization objects:-

S_BTCH_ADM:- Full access to user (Admin) (fields:- BTCADMIN).

S_BTCH_NAM:- check for particular user (fields:- BTCUNAM).

S_BTCH_JOB:- Apart from scheduling other jobs will be accessed by user (fields job group□, job action□).

***

Merging Tables:-

SQVI:- This T-code helps to merge two tables.

To avoid SQVI

SUIM → User → user Address by Address data (same info can be pulled from this).

Note: We can schedule this as Background job also (SQVI (program → execute → Background job)).

Ecatt Scripting:- Scripting for SUIO.

SECATT:- This T-code helps to perform Test script and Test configuration and also uploading file job.

Provided Notes

Major Versions of SAP:-

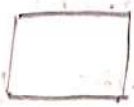
1. 4.6 C
2. 4.7 EE (Enterprise edition)
3. ECC 5.0 (Enterprise core/central component)
4. ECC 6.0
5. SAP ERP 6.0 is the current release and new.

* Functions are imported via (EHP)

Enviornments in SAP:-

Development

Quality



Production.

Development Enviornment:-

→ Development enviornment (Dev) is where programmers and consultants carry out the customization of the ERP functionalities based on the company's requirement.

→ Basically it is where changes are orginally made.

→ Once developers and consultants have programmed and configured all changes in the development server, they transport this data in the form of transport request to the test server (Quality).

Quality Enviornment (QS):- Is where the core team members and other staff test the customization of the software designed and programmed.

* In this testing server, testers check the programs before trans-porting them to the production servers, it is an acceptance or rejection decesion.

* Users can also request for changes if a transaction (or) program (or) role has not been ~~developed~~ developed correctly.

Production Enviornment:- Is where the real time data of the company is recorded and stored. (7)

* Every transaction and business process that is performed by end users (client) will be run and go live.
* Client data such as transactions, programs, interfaces, roles will be transported into the production enviornment once it has overcome the previous stages (DEV & QAS).

Note:- In order to have real data without misconfigurations in the production enviornment, it is important that every piece of data is transported after being tested appropriately in the Quality enviornment so we can guarentee the integrity and consistency of the transactions running in PRD.

Landscape:- SAP system landscape is the group of systems you have installed, all the systems are linked to different transport routes to main system.

* System landscape may vary from company to company (or) business to business.

3-System landscape:-

→ SAP recommends a 3-system landscape in which each of the central clients has its own SAP systems.

→ This consists of a development system DEV, a quality assurance system QAS and a production system PRD.

→ The development system contains the customizing client CUST, the quality assurance system contains the quality assurance client QTST and the production system contains the production client PROD.

SID in SAP:- System Identifier (SID) is a unique combination of three letters used to identify a SAP system. (2)

* SAP ~~can~~ SID can be all letters or atleast one letter followed by 2 letters (or) digits.

* There are no specific instructions to name the SID expect it should be

3 charectors and in Uppercase.

Examples for SID's: R3D, R3Q, R3P (or) D50, Q51, P53.

SID's in SAP:-

Flavours in SAP:-

1) IDES :- are pre-customized systems and they contain sample data used for training. IDE's systems support 62 languages.

2) Non IDES:- System contains Business data. Non-IDES system supports only few languages.

IDES :- Internet Demonstration & Evaluation System

Clients in SAP:- One of the most basic concepts in SAP is that of "client".

* A client is defined as a legally and organizationally indepen-dent unit within SAP R/3.

client is used to seperate data.

* SAP R/3 comes inbuit with three standard clients viz. 000, 001 and 066 in Non-IDES and contains extra client 800 in IDES.

Clients in SAP:-

* Clients 000:- Contains all standard configurations, parameters, standard transactions, etc that are normally used in the SAP R/3 business enviornment.

* Client 000 is called as Golden client.

→ It is used as a source to create new clients.

* Client 001:- Client 001 is a copy of client 000.

→ It is also called as backup of Golden client.

* Client 066:- This is also called as early watch client.

→ This client is purely a service client that enables SAP to access remotely the customer system with regard to analyzing errors and performance.

* client 800:- is the IDES client.

It contains IDES sample data to use it for the customers.

Default users in SAP:-

The SAP system come with several default users that have extended access to the system. These users are created during the installation process and through the implementation and customization of certain functionally. When you install an SAP system standard users like SAP*, DDIC & EARLY WATCH are created.

User	Description	clients	Default Password.
SAP*	SAP system super user	000, 001, 066 and all new clients	060719992 and "PASS".
DDIC	ABAP dictionary and SW logistics super user.	000, 001	19920706.
Early watch	Dialog user for the SAP early watch alert service in client 066	066	support
SAPCPIC	user for remote connections	000, 001, 066, and new clients	ADMIN.
TMSADM	user for TMS	000	set during installation.

Risk with default users in SAP:-

Like a lot of other application software, SAP comes with a number of generic accounts. These are intended to be used for initial installation and setup purposes. and their passwords are well known.

* It is therefore critical that these id's are secured once the initial setup activities have been completed.
* The passwords of these generic ID's should be reset; and the high-privileged profiles (SAP_all & sap_new) should be removed.

Checking default Users in SAP:-

The standard Report RSUSR003 displays standard users and their statuses across all clients in a system. It's important to execute this report in each system because users are client

- dependant and hence different in each client & system. (1)

* Depending on your current release, report RSUSR003 might not report user TMSADM.

User administration:-

Introduction to User Id:-

→ User Identification (USER Id) is a logical entity used to identify a user on the SAP system.

→ User Id's are client-dependant & stored in table USR02.

→ To access different clients, the user must be created in each client seperately. passwords are also client-dependant.

→ SAP user Id's can be up to 12 charectors long. Using the full length makes it easier to identify users.

User Id naming convention:-

Defining a naming convention for your users is very important and helps reduce complexity in the long run.

* With a proper naming convention, you can easily identify your users, which allows you to use the selection criteria more precisely.

User administration using 'SU01':-

The central transaction to create and maintain a user is Transaction SU01.

* With transaction SU01, an administrator can create, maintain, and delete users, as well as change their properties and parameters, assign roles and profiles, change logon data, and more.

* To create a user, you have to define a user Id of no more than 12 characters in length.
* User Id's should follow a naming convention so that identifying them later is possible.

Important Tabs in SU01 :-

Documentation (present in 's).	Free from text to capture doumention regarding the user
Address	Information about the user.
Logon Data	Password, usertype, and validity for the user.
Defaults	Defaults values for the user.
Parameters	Standard field defaults
Roles	Role assignments to the user.
Profiles	Profile assignments to the user.
Groups	Assignment to user groups.
Lic. Data	Classification for measurement.

Mass User changes Using SU10:-

* The easiest and quickest method for maintainence of multiple users is provided by the SU10 transaction.
* The limitation with Transaction SU10 is you have to perform the change for all users in the selection. Individualization is not possible, nor can you assign a different set of roles to several users
* There are two steps involved in Transaction SU10. They are:
  - → Mark the user selection and
  - → Mark the adjustments to the users.

Caution Note:- One of the most common and costly mistake is to click the delete button to remove users from the selection. (8)

* The delete button will be immediately and irreparably delete all users that are in the selection. No return or revert button is available.

User Groups:-

* User groups are used to categorize users into common logical groups.
* You can use the user group to segregate user administration, but also to search and sort users by a common grouping.
* To create and maintain user groups, user Transaction SUGR. Using this transaction, you can create, edit, display, and delete user groups from the system.
* User groups are created in each individual system. User groups cannot be transport them across your SAP landscape.
* Table USGRP is the master data table for user groups and USGRPT is the text table.

Default User Group SUPER:-

* The SUPER user group has a special status in the predefined user profiles.
* The users that are assigned to group super can be maintained (or) deleted only by the new super user that you define.
* Note:- Assign all user and authorization administrator user Id's, Basis User Id's and standard users to the group SUPER.

User lock status:-

In the user master table (table USR02) there are different lock statuses of the user in the UFLAG field. The following statuses are known to an SAP system.

* 0 : User is not locked.
* 32 :- User is locked globally by an administrator
* 64 :- User is locked locally by an administrator.
* 128 :- User is locked due to incorrect logons.

* The different lock statuses let you identify how the user was locked.

Mass Locking of Users:-

Use the transaction code EWZ5 (or) EWZ6, or execute program EWULKUSR in SA38 to mass lock/unlock id's in the ECC system.

Note * Transaction codes EWZ5 and EWZ6 do not exist in any other SAP system except ECC.

User types in SAP:-

The SAP system categorizes users into several types for different purposes. These are the different types of users available in SAP.

1. Dialog
2. System.
3. Communication
4. Reference and
5. Communication Service.

1. Dialog User:- Individual system access (personalized)
   → Logon with SAPGUI is possible.
   → The user is therefore interaction capable with the SAP GUI.
   → Expired (or) Initial passwords are checked.
   → Users have the option of changing their own passwords.
   → Multiple Logon is checked.

Usage:- for individual human users (also Internet users).

* Execute - F8.

2) System User:- System dependent and system-internal operations.

→ logon with SAP GUI is not possible. The user is therefore not interaction-cable capable with the SAP GUI.

→ The passwords are not subject to the password change requirement that is, they cannot be initial or expired.

→ Only an administrator user can change the password.

→ Multiple logon is permitted.

→ Usage:- Internal R*C, Background jobs processing, External RFC.

* RFC - Remote function Call.

3. Communication User:- GUI is not possible

* Users are allowed to change password through some software in middle tire tier Individual system access (personalized).

Usage:- External RFC.

Drawback:- # By the help of external third parties passwords can be changed by this.

4. Service User:- GUI logon is possible

→ Initial password and expiration of password are not checked.

→ Multiple logon's are allowed.

→ Users are not allowed to change the password.

→ Only admin can change the password.

Usage:- Anonymous system access (for example, public web services).

5. Reference User:- GUI login is not possible

→ Initial password and expiration of passwords are not checked.

→ The assignment of reference users to users can be checked in the table USREFUS.

* Reference user is assigned to a dialog user from SU01 → Roles tab..

→ For 1 Dialog User, only 1 Reference User can be assigned.

Usage:- Primarily assigned to dialog user for authorization enhancement.

Introduction to System Profiles:-

→ One of the most fundamental tasks of configuring any SAP system is setting profile parameters.

→ Profile parameters control many aspects of the system's behaviour and operation. Many settings that are crucial to the security of the SAP system are set using profile parameters.

→ Profile parameters, often referred to as system parameters, are individual system setting that an administrator is able to set.

→ Collection of these system Parameters is called a profile.

Understanding System Parameters:-

→ System parameters can be thought of as basic operating instructions for ~~ow~~ your SAP system. These instructions tell the system things like how much memory to allocate to a work process, how to negotiate secure connections, even how many times a user can try a password before that user's account is locked.

→ System parameters resides both in the database and on the OS. The reason for this is that when the administrator can't login to the system due to it being down, incorrectly configured, or in an error state, he can still login to the OS and manually change before startup is attempted.

→ Although this is fine in an emergency cases, in regular situations an administrator should always use the SAP system to change parameters for proper change tracking and control.

Understanding System Parameters:-

→ There are two advantages of keeping profile parameters in the database.

1. Multiple versions can be easily kept:- The active version is used, and inactive versions can be kept for historical reference or even reactivated if the need arises.

2. Changes can be tracked more easily by SAP user ID rather than the OS administrative use ID, SIDADM.

Therefore, many auditors requir that profile changes only be allowed using the proper transactions in the system.

System Profiles:- It can be defined as a collection of parameters intended to define the behaviour of the system.

There are three types of system Profiles - They are:

1. Start Profile:- Define the start procedure of the Instance.
2. Default Profile:- Applies to all the instances within the system.
3. Instance Profile:- Applies to a single Instance.

Note:- From SAP Net Weaver 7.5 onwards, the contents of the start profile can now be found in the instance profile. This change was for simplicity because two independant profiles weren't really needed.

Parameter Structure:- login/min_password_lng = value

- login → Application area
- min_password_lng → Name of the parameter

1. The application area:- This tells you the group that the parameter belongs to. for example, a parameter with a "login" application area will have something to do with user authentication and logon. The application area is always followed by a foward slash (/).

eg:- login/.

2) Name of the parameter:- This is a descriptive name used to briefly describe what the parameter does.

3. The value:- is seperated from the rest of the parameter by an equals sign (=).

* putting all this together, a parameter looks like.

login/min- password-digits = 6.

Static Vs. Dynamic Parameters:-

These are the two types of profile parameters in an SAP system.

Static Parameter:-: Are evaluated once at system startup. changing these parameters during running operation will have no effect on the system. The system must be restarted for these profile parameters to come into effect.

Dynamic Parameters:- Changing these parameters during running operation will affect the system immediatly as these profile parameters doesn't require a restart to come into effect.

Security Policy:- T-code:- SECPOL

from release 7.40 SP8, SAP introduced security Policies to define user-specific security parameters, contrary to the system profile values.

* The transaction SECPOL is used to maintain the security policies and the security Administrator has the option of defining as many policies as you wish.

* The security policy can be assigned to the user from Logon Tab using SU01.

* Security policies

Caution!- Security policies do not override individual profile values, but replace all values. (19)

The values that is not defined in a Security Policy are not set to the secure values according to RZ10 parameters, but to insecure kernel values in user context. Thus, you can inadvertently weaken secure values such as login restrictions and password complexity.

	Value			
profile parameter	kernel	Profile	SECPOL	User
login/min_password_lng	6	10	8	8 → min password length.
login/min_password_lowercase	0	1	-	0 1
login/min_password_uppercase	0	1	-	0 1

Password Poli Blacklist :-

In table USR40, which can be maintained through transaction SM30, password blacklist can be defined such as that they can't be used as productive passwords. To maintain table USR40, there are two wildcards

→ ? stands for a single character.

→ * stands for a sequence of any combination of characters of any length.

* You can also define a password as case-sensitive, but mostly it doesn't make sense to force case-sensitive because a blacklisted password shouldn't be possible to choose if a single character is set uppercase

Password Policy:- The password policy may be set by your IT policy, or you may be setting the policy by yourself.

→ Password policies are necessasary to protect the confidentiality of information and the integrity of systems by keeping unauthorized users out of computer systems. The fundamental protection of computers and networks (the password) is still in use.

→ Most users will do what's easiest, which can lead to easy-to-guess passwords that can result in serious security breaches. Therefore, make sure that you enforce strong passwords through the login parameters.

→ Many password policies specify attributes and procedures for handling user passwords, Among these attributes are: minimum length, allowed charcter set, disallowed strings (all numbers, dictionary words, variations of the username (or Id), and the duration of use (expiration) of the password.

Important Login Parameters:

Parameter	Description	Recommended value
login/min_password_lng	Minimum Password length	10.
login/min_password_letters login/min_password_digits login/min_password_specials	Minimum number of letters, digits, and special charcetors in a password	2
login/min_password_lowercase	Minimum lower case letters	1
login/min_password_uppercase	Mininum upper case letters.	1
login/min_password_diff	Minimum charcetors that must be different from the previous password	4
login/password_history_size	Sets the number of different passwords so that the same password can't be used again	20.
login/password_change_waittime	Sets the time in days until the password can be changed again	1

Quick Tip:- If the security consultants would like to view logins Parameters set in the system, it can be checked using the t-code

RSPFPAR - LOGIN.

Logging Table changes:- rec/client → OFF. / All client.

* SAP offers the option of logging changes to tables. Table logging is primarily used to record changes to customizing data.
* This will help in tracing which users changed data records in the tables, when added or deleted. For logging master and transaction data, the change documents are used.
* By default, around 40,000 tables are already available in SAP ERP or SAP S/4 HANA for which logging provided.
* In particular, the customized tables with accounting - relevant contents must be logged as well as the SAP standard tables.

Pre-requisites for logging Table changes:-

There are two pre requisites for logging changes to a table. They are:

1. Logging must be enabled using the parameter rec/client, and
2. Logging should be activated for the table for which logging is needed, (using SE13 T-code).

Once the logging (SCU3) is activated, The log records are stored in table **DBTABLOG**. → To view table (T-code).

* By default, no table changes are logged. This must be explicitly activated. Activation takes place via the system parameter rec/client. The parameter can contain the following entries:

OFF = Logging is deactivated.

ALL = Logging is activated for all clients in the system.

<client number>, [...] = only the specified clients (maximum ten) are logged

eg:- <client number> = 810, 800, 850. —— 10 entries

All other entries (e.g. ON) means: Logging is deactivated. (7)

* A special feature is the logging of cross-client tables. Changes to these tables are logged in all clients of the system, as soon as at least one client is defined in the parameter rec/client.

Eg:
* In the production system with the setting rec/client = 100 ensures that changes to cross-client tables in all clients of the system are logged.

* Activate the technical settings of the table - you can do this in transaction SE13.

Checking the Table log:-

→ The table changes log is available via transaction SCU3.

→ The changes will be logged in a table DBTABPRT.

→ SAP recommends that you activate the logging of changes to table data for those tables that are critical or, susceptible to audits.

Monitoring the tables that are not locked, logged.

The report RSDBPRCHK or, transaction RSDBPRCHK_AUDIT check tables & regarding the table logging settings.

→ If you care about high-profile tables, such as critical IMG configuration tables, you can use the table log to get an understanding of how the table is being changed and who are the people making the changes.

Note:- Logging can have a significant impact on performance; it should be performed on an as-needed basis.

Types of Data in client:-

There are two types of data existing in a client. They are

1. client Dependant and.
2. client -Independant.

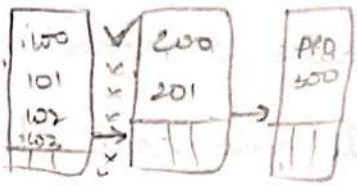
→ Client independant objects or tables are common for all clients. On the other hand, client dependent objects are never shared with other clients.

Client dependant Database Tables:- MANDT field:-

The technical table field that denotes a client is the MANDT field. This field is present in all client-dependant tables. client-independent tables don't have a MANDT field and represent any and all clients. Use care when changing client-independant tables as they affect all clients.

Client Independant Change:- If a change is made in Dev 100, the change is reflected in all clients of Dev. (USR40 table example).

Client Dependant change:- If a change is made in Dev 100, the change is reflected to that particular client (eg:- user).



Client Settings:- It's important for a security administrator to know and understand the different possible clients settings and what they may be used for.

To check client settings in the system, follow these steps

1. Navigate to Transaction SCC4.
2. Double click the client you would like to view.

Client Role:-

Possible choices are as follows:-

Production:- For the active use of the business users. It's essential that no changes are made in this client.

Test:- Developers use this client setting to test their customizing settings and workbench developments.

Customizing:- For the creation of customizing settings and workbench developments.

Demo:- for demonstration or prototyping purposes.

Training / Education:- Typically used to train users on change before import into production.

SAP Reference:- clients used by SAP.

* Changes and Transports for client Specific Objects:-

These options cover changes to client-specific objects and how they're transported using the transport system. Possible choices are as follows:

Changes without automatic recording:- This means that changes in the customizing settings of the client are allowed: They aren't automatically captured in a transport for moving to other systems or clients. Changes can be manually transported to other clients or systems.

Automatic recording of changes:- This means that changes to the customizing settings of the clients are allowed. They are automatically captured in a transport for moving to other systems or clients.

No changes allowed:- changes to the customizing settings of the client aren't allowed with this setting.

Changes w/o automatic recording, no transports allowed:- Changes are allowed to the customizing settings of the client but may not be transported with the setting.

* Cross-client object changes:- These options cover changes to cross-client objects and how they're transported using the transport system. Possible choices are as follows:-

Changes to repository and cross-client customizing allowed:- There are no restrictions on the changes of cross-client objects for the client when this setting is used. Both cross-client customizing objects and objects of the SAP repository can be changed.

No-changes to cross-client customizing objects:-
Cross-client customizing objects can be changed in a client with this setting.

No changes to repository objects:- Objects of the SAP repository can't be maintained in a client with this setting.

No changes to repository / cross-client customizing objects:- Combination of both previous restrictions.

CATT and eCATT Restrictions:- This setting either allows or restricts the computer-Aided Test tools (CATT) and enhanced CATT (eCATT), which are scripting utilities used for automated testing. This setting either permits these scripts to run or prevents them from doing so.

Restrictions:

Locked due to client copy:- This check box will indicate when the client is locked against logon. It's used during a client copy to prevent data changes during the copy. It's not a selectable box because it only indicates status.

Protection against SAP upgrade:- This checkbox will prevent an upgrade from taking place on this client when the system itself is being

upgraded. It's only used in exceptional cases.

Settings Recommended in the Dev clients :-

→ Client Role :- Customizing.

→ Changes to client-specific objects :- Automatic Recording of Changes

→ Changes to Repository and cross-client objects :- Changes to Repository and cross-client allowed.

→ Protection level :- Protection level 1

→ E-catt settings :- E-catt and CATT allowed.

Settings Recommended in QAS clients :-

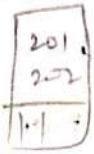
→ Client Role :- Test

→ Changes to client-specific objects :- No changes allowed.

→ Changes to Repository and cross-client objects :- Changes to Repository and cross-client not allowed.

→ Protection level :- Protection level '0'.

→ E-catt settings :- E-catt and CATT not allowed.



Settings Recommended in ~~Pro~~ PRD clients :-

→ Client Role :- Production.

→ Changes to client-specific objects :- No changes Allowed.

→ Changes to Repository and cross-client objects :- Changes to Repository and Cross-clients not allowed.

→ Protection Level :- Protection level 1/2.

→ E-catt settings :- E-catt and CATT not allowed.

Client Logon Locking :- Occasionally, you'll need to lock a client. This may be for an upgrade or a system maintainence activity. Locking the client will prevent users from logging into the client that is locked. To lock a client, Proceed with the following steps:

→ Navigate to Transaction SE37:

→ Enter the function Module name "SCCR_LOCK_CLIENT" and click the Test/Execute button in the tool bar.

⇒ Enter the number of the client for which you'd like to prevent logon. Check the execute button in the toolbar.

Introduction to Central User Administration (CUA) - SAP:-

* In a large landscape consisting of number of SAP systems, it becomes time consuming job to perform user administration. For instance, if one needs to assign the role to one user in all the systems involved in the landscape, one needs to perform the below steps on each system in landscape:

  a) login to system.

  b) Execute the t-code SU01 and open the user

  c) Assign the role and save the changes.

* The above process can be simplified if Central User Administration System (CUA) has been installed in the above landscape. Using Central User administration, you can maintain user master records centrally in one system.

* changes to the information are then automatically distributed to the child systems. This means that you have an overview in the central system of all the user data in the entire system landscape

* One system in the Central User Administration ALE environment is defined as the central system.

* The central system is linked with every child system in both directions.

* The child systems are not linked to each other, with the exception of the central system, which is itself a child system, from the point of view of Central User Administration.

Benifits of Central User Administration :-

* Once you configure CUA users can only be created or deleted in the central system.
* The central system is linked with every child system in both directions.
* The child systems are not linked to each.
* User attributes can be maintained only locally, only centrally or both centrally and locally.
* So, the required roles and authorizations must exists in active form in all child systems.
* As a result each user only has to be administered once centrally which gives the administration a much clearer overview of all users and authorizations.

Steps for configuration of Central User Administration :-

1. We need a SAP Landscape / Single system with multiple clients.
2. Decide the Parent System and child systems.
3. Create logical systems and assign logical systems to corresponding client.
4. Create communication User in central system and child system.
5. Create RFC connections between systems.
6. Create model view and attach child systems to the Parent System.
7. Define Field Parameters.
8. Transfer Users from child systems to Parent Systems.

→ The administrator should have access to SAP and t-codes SU01, BD54, ~~BD64~~, SCUL, SCUA, SCUM, SM59 to configure central User Administrations.

→ Roles to be assigned will be found in Running Notes (CUA topic).

Setting up Field Distribution Parameters (SCUM):-

* If you are using Central User Administration, you can use the distribution parameters in transaction SCUM to determine where individual parts of a user master records are maintained.
  - → In the central system.
  - → Locally in the child system.
  - → In the child system with automatic redistribution to the central system and the other CUA child systems.

* Every input field of the user maintenance transaction SU01 has a field attribute, that you set once in the central system with transaction SCUM during Customizing. As far as possible, you should then not change the field maintenance indicator at all.

Different Attributes for Field Distribution Parameters (SCUM).

Globally:- You can only maintain the data in the central system. The data is then automatically distributed in the child systems. These fields do not accept input in the child systems, but can only be displayed. (Most times we go for this).

Proposal:- You maintain a default value in the central system that is automatically distributed to the child systems when a user is created. After the distribution, the data is only maintained locally, and is not distributed again, if you change it in the central or child system.

Ret Val/Redist:- You can maintain data both centrally and locally. After every locally change to the data, the change is redistributed to the central system and distributed from there to the other child systems.

Local:- You can only maintain the data in the child system. Changes are not distributed to other systems.

Everywhere:- You can maintain data both centrally and locally. However, only changes made in the central system are distributed to other systems, local changes in the child systems are not distributed.

Report RSDELCUA in CUA:-

* You can remove central user Administration (CUA) again, simply by performing the reverse of the setup first in the central system and then in all child systems.

→ The first three steps (transactions SCUM, SCUM & SCUA) are combined in the report RSDELCUA.

→ To delete CUA, logon to the central system Run Report RSDELCUA from SA38.

Purpose of text comparision in CUA:-

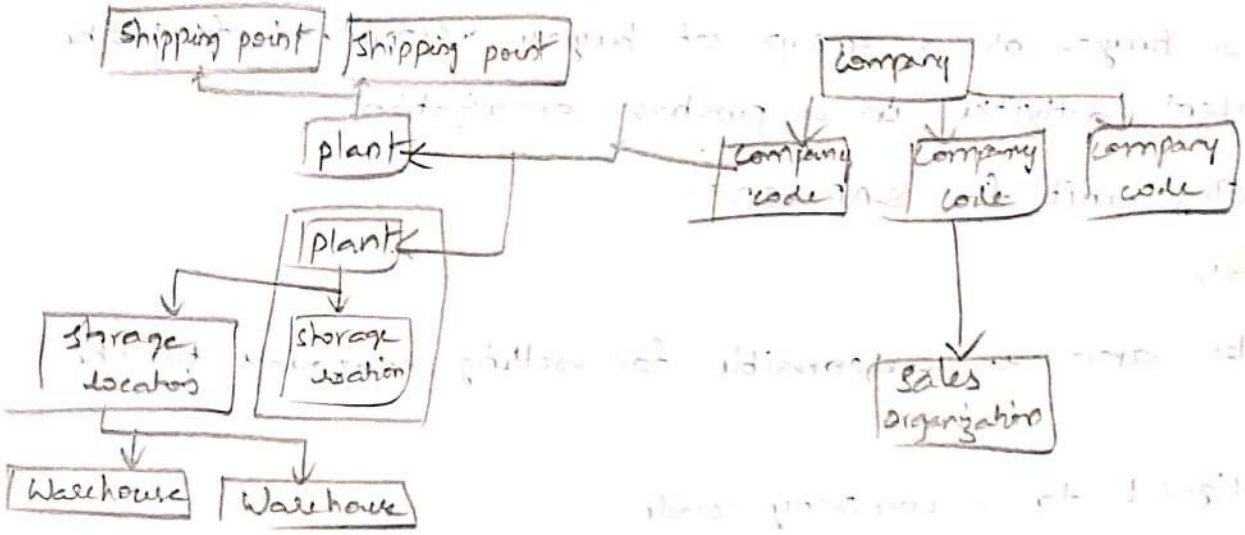
→ Existing roles are still maintained and new roles are still built in the child systems.

→ To be able to assign users in the central system the roles and profiles defined in the child system, there is the text comparision button in the Roles and profiles tab pages in the central system together with their short texts.

→ The names of the roles and profiles are available in the central system in the value help (f4 help). Since the information in the child systems might change, you should occasionally repeat the text comparision.

Enterprise Structure in SAP:-

* Organizational units are interlinked in a specific way to enable effective functioning of enterprise/organization.
* This is referred to as enterprise structure.



Relevant Org units for SAP MM:-

Plant:-

* plant is an organizational unit within a company where activities take place.
* A plant will produce goods and makes goods available for the company.
* In the system, the plant is assigned to exactly one company code.

Storage location:-

* Storage location is an organizational unit, which actually differentiates between different material stocks in a plant.
* storage location is a place where stock is kept physically.
* A plant can consists of multiple storage locations.

Relevant Org Units for SAP MM:-

Purchasing Organization :- A purchase organisation is an organizational unit under a company or a plant that is responsible for the external procurement.

* A purchasing organization can be

(2*)

Purchasing group:-

* Purchasing group is an organizational unit responsible for the everyday procurement activities within an organization.
* It is a buyer or a group of buyers responsible for the procurement activities in a purchase organization.

Relevant Org units for SAP SD:-

Sales Area:-

The sales area is responsible for selling materials to the customers.

→ It's assigned to a company code.

Sales Organization:-

→ All sales documents are assigned to the sales organization.

→ One or more sales organizations can be assigned to a sales area.

Distributional channel:-

* The distributional channel is the way materials and services reach the customers.
* Typical distribution channels are wholesale trade (business-to-business [B2B]), retail trade (business-to-consumer [B2C]), and mail orders to or direct sales.

Division:-

Similar products are combined in a division - that is, a grouping of materials and services that are distributed by the business - which organizes the responsibilities for these products within business.

Shipping point:-

→ The shipping point handles shipping

→ They may be physically detached from the business (eg. loading ramps (or) airports.

Technical Names of the Org. Units:-

Org Unit	Technical Name.
Company code –	BUKRS
Plant –	WERKS
Purchase Organization –	EKORG,
Purchase Group –	EKGRP
Sales Organization –	VKORG.
Sales Group –	VKGRP
Division –	SPART
Distribution channel –	VTWEG
Shipping point –	VSTEL
Storage location –	LGNORT
Sales office –	VKBUR.

Important Tables Related to Org. Units:-

Org. unit	Table Name.
Client –	~~T000~~ T000
Sales Organization –	TVKO
Distribution channels/ Sales organization –	TVKOs
Sales Area –	TVTA
Company code –	T001
Plants –	T001W
Storage locations –	T001L
Distribution channel –	TVTW
Purchase Organization –	T024E
Purchase Group –	T024.

Master Data and Transaction Data:-

Master Data:- Most software systems have lists of data that are shared and used by several of the applications that make up the system. This is called Master Data.

→ This master data is often one of the key assets of a company.

→ In fact, it is not unusual for a company to be acquired primarily for access to its customer Master Data.

→ The four General Master Data Domains are:-

1. Customers (Customers, Employees, Sales Persons).
2. Products (Materials, Parts, Store and Asset).
3. Locations (office Location and Geographic division).
4. Other (Contracts, Warranty, License etc.).

Master Data in Procure to Pay:-

1. Material Master
2. Vendor Master and 3) Purchasing Info Records

T-codes Related to Material Master (Important):-

MM01 – Helps to create Material Master.

MM02 – Helps to change Material Master.

MM03 – Display Material Master.

Vendor Master:

XK01 – Create Vendor Master.

XK02 – change Vendor Master

XK03 – Display Vendor Master

Purchase Info Master:-

ME11 – Create Purchase Info Master.

ME12 – Change Purchase Info Master.

ME13 – Display Purchase Info Master.

→ Master Data in order to Cash

→ Material Master

→ Customer Master and

→ condition Master Records.

→ Important Tcodes Related to Order to Cash Master Data:-

Customer Master:-	Condition Master:-
XD01 - Create Customer Master.	VK11 - Create condition Master.
XD02 - change customer Master.	VK12 - Change condition Master.
XD03 - Display customer Master.	VK13 - Display condition Master.

Transaction Data :- Transaction data is used by the Master Data. Assume a scenario of purchasing a product: Data such as price, discounts, and method of payment are considered as transitional data.

→ Transactional data always changes, for example, the price of the purchased items can be $100 on one day and $200 on another day. In other words, the transaction data is highly volatile.

Q) What will happen in background when t-code is executed.

A) TSTC:- System checks weather the t-code is valid or not in table TSTC.

SM01:- System checks weather the t-code is locked or not using sm01.

S-Tcode:- System checks weather tcode is exists against to field TCD under authorization object, S_Tcode (OS), not.

Authorization objects:- System checks weather t-code is having any relevant authorization objects or not.

* If there are any, again system checks weather user is having access to those relevant authorization objects or not.

→ If any one of the checks failed, then system will not allow to execute the transaction.

→ If all the checks are passed, system checks in the ABAP program (that is called in backend when t-code is executing), is there any authorization object (or) values are maintained against "AUTHORITY_CHECK" command.

Profiles:-

Maximum No. of Profiles assigned to a User — 312

Maximum No. of profiles in a role — 101

Maximum No. of fields in a Profile — 150

Authorization Object:-

Maximum No. of Auth object — 10

Maximum No. of fields in Auth. object — 1

No. of fields Mostly available in a Auth. object — 2.

Roles:-

Maximum no. of Roles Assigned to a User — 312.

Maximum no. of fields in a Role — 15150.

Maximum Length of a Role Name — 30

Maximum No. of T-codes in a Role — 14000.

Users:-

Maximum length of a User Id — 12

Maximum length of Alias Name — 40.

Maximum No. of Profiles Per user:-

Since the first two characters are for the change indicator → The Maximum no. of profiles that can be assigned to a user is 312.

→ The relationship between user and profile can be seen in table USR04. The PROFS field is used to save the change indicator

(C = User Created), M = User changed) and the name of the profiles assigned to the user.

→ The PROFS field is defined with a length of 3750 characters.
→ Since the first two characters are for the change indicator, 3,748 characters are still available for the list of profile names per user.
→ Since the maximum length for each profile name is 12 characters, the maximum number of profiles per user is 312.

Roles:-

A role contains all the authorization objects and field values.
→ Role will define the job function of a employee in an organization.
→ User might, however, have more than one job/position.
→ Such a user will be assigned multiple single roles.

Profiles:-

Profiles existed long before roles
→ In versions before R/3, profiles were used to authorize users to the system.
→ When a role is generated, it created a profile that contains the actual authorization values.
→ A profile can hold a maximum of 150 authorization fields.
→ Profiles are still available and can be used to authorize user.

Object class:- An object class is a grouping of Authorization objects.
→ It may contain one or more than one authorization objects.
→ You can see all the available object class in Transaction SU21.

Note:- The list of all object class available in the system can be accessed from the table TOBC.

Authorization Object:- SAP offers a wide range of authorization objects to protect and limit access to certain applications.

→ Authorization objects contain a minimum of 1 and a maximum of 10 fields with maintainable values. In most cases, an authorization objects consists of two fields: one is the activity field and the other the objet to be protected.

→ You can see all the available authorization objects in Transaction SU03 (or) Transaction SU21.

→ You can also create and maintain customer-specific authorization objects with SU21 (or) SU03. This requires a developer key because it's a development-specific task.

Note: To get a list of all authorization objects with the available authorization fields, go to table TOBJ.

Authorization Object Naming Convention:-

→ The first letter of SAP authorization objects is intelligently coded to represent the SAP module for which it belongs.

Ex: M_MATE_WRK belongs to the module Materials Management.

A	Assets Accounting	L	Logistic execution
F	Financial Accounting	M	Material Management
G	Special Ledger.	P	Human Resources.
K	Controlling.	S	Basis & Security.
V	Sales & Distribution		

Activities in SAP:- A complete list of activity values and their meanings can be found in SAP Table TACT. Some of the Activities are: 01, 02, 03, 05, 06, 04, 16, 27, 43 → Release.

Create, Change, Display, Lock/unlock, Delete, Print, execute, enter, assign, include, assign, execute, ...

Generic Maintainance in a field:

Field value	Type	Meaning
*	Generic	All values
A*	Partly generic	All values starting with letter 'A'.
AAA	concrete	only the value "AAA".
*A		not effective
A*A		not effective.

Traffic Signals:- ○○● (Green) → Authorization field contents maintained. (24)
yellow ← ○●○ → Some unmaintained authorization field contents.
red ← ●○○ → Unmaintained organization levels.

Different Authorization Status:-

1. **Standard:-** The object and its authorizations come from Transaction SU24.
2. **Manually:-** The object was manually introduced to the role. There is no reference to which object it belongs.
3. **Maintained:-** The object and its authorizations come from Transaction SU24, and open authorization were maintained by the administrator.
4. **Changed:-** The object and its authorizations comes from Transaction SU24, but the administrator changed the automatic proposals.

User Buffer:- The user Buffer (Transaction SU56) contains all authorizations that a user is authorized for.

→ The user buffer is filled during the logon procedure and remains active until the user logs out or restarts the SAP menu (command /n).

→ As an administrator, you can also check the user buffers of other users in the system by clicking the Display for other user/authorization object button and entering the user ID.

→ To Reset user buffer for a specific User, Use the t-code SU56 and if user Buffer should be reset for all the users, execute the report RSUSR406

Checks Performed when a T-code is executed:-

The system checks in table TSTC whether the transaction code is valid and weather the system administrator has locked the transaction.

→ The system then checks whether the user has authorization to start the transaction.

* The authorization object S_TCODE (transaction start) contains the field TCD (transaction code). The user must have an authorization with a value for the selected transaction code.

⇒ If an additional authorization is entered using transaction SE93 for that transaction need to be started, the user also requires the suitable defined authorizations object (TSTA, table TSTCA).

→ The system checks whether the transaction code is assigned an authorization object. If so, a check is made that the user has authorization for this authorization object.

Manually inserting objects is not at all recommended :- (Caution)

Not only is there no reference to a transaction (because it doesn't get pulled from Transaction SU24), but most likely manually inserted authorization will result in orphaned and unmanagable roles and authorizations.

Organizational levels:- Oraganizational values, or org values, authorize a user based on enterprise structure.

→ Service B. Several business transactions require certain org values to function.

→ When the Org. Values is maintained in Org. level for a role, the data gets stored in the table. AGR_1252.

→ Org values are maintained as a header-like set of data that is valid for the whole role. Once maintained, all authorization objects that require an org field will get the data proposed from the header.

Note:- If the org. level is not maintained in the traffic signal "RED" it will be shown against the corresponding field.

Few examples of Org levels:-

→ Company code – $BUKRS
→ Plant – $WERKS
→ Purchase organization – $EKORG
Sales Organization – $VKORG
Purchase Group – $EKGRP.

Derived Roles:- Composite Role:- A composite role is a container which is a collection of single roles.

→ The advantage of composite role is you can indirectly assign multiple single roles to a user by assigning only the composite role that contains the single roles.

→ Composite role doesn't have a profile on its own. Since Composite Role doesn't have a profile on its own, we can't add a composite role to composite role.

→ Relationship between a Composite Role and a Single Role can be seen in the table AGR_AGRS.

Derived Roles:- As the name indicates, roles are derived from already existing roles.

→ The concept of parent and derived roles was introduced by SAP to simplify role administration tasks.

→ Its specially helpful while it mapping security for large enterprise spread across multiple geographies and(or) divisions.

→ A child role derived from a parent role will have all attributes (transaction/ authorization object values) same as it parent except the values of the Organizational level fields (plant, company code, sales organization).

→ Roles derived from another cannot have any additional menu entries. The menu is maintained in the master role which take effect immediately in all derived roles.

→ To change the menu of the derived role without changing the menu of Referred role you have to break the inheritance relationship

→ The relationship between parent role and child role can be seen in AGR_DEFINE table.

Note! Once the relationship breaks, the derived role is dealt as a normal role and the into inheritance relationship cannot be re established.

Introduction to SU20 and SU21:-

→ Often a security administrator comes across requirements where the existing authorization objects delivered by SAP is not enough.

→ Mostly these come during custom developments through completly new program or enhancements to existing SAP programs.

→ In such situations, SAP provides us with the option of defining completly new authorization objects

→ The names of these customer specific objects should begin with 'Y' (or) 'Z' and can be crated through the SU21 transaction. If required, we can define new authorization fields as well through the transaction SU20.

→ Using transaction SU21, an individual object classes and the authorization objects contained in each class is displayed. The following values are displayed for one object:

1) Basic Data 2) Authorization fields 3) Documentation & 4) Permitted Activities.

Mass Generation of Profiles:-

The Mass profile generation transaction (SUPC) can be used to determine which roles already have authorization profiles.

→ SUPC can also be used perform a mass generation of roles or generate the missing role authorization profiles for role in the background.

→ The mass generation program allows selection in the initial selections the program will only display the findings and you can manually decide if you want to generate the profiles or) you can go with automation.

→ You will need the following authorizations to use transaction SUPC.

- User master maintainence: Authorization Profile (S_User_Pro)
- User master maintenance: Authorizations (S_User_Aut)
- Authorization system: check for roles (S_User_AUR)

→ The following status of the profile can be seen in SUPC based on which decision to generate profiles or not can be decided.

* No profile name exists.
* No current profile
* No authorization data
* Profile generated.
* To be compared.

Regenerating of SAP_ALL Profile:-

→ The SAP_All only contains the authorizations that were available in the system at the time of the last generation. If new objects are imported through a software extension or) update, this leads to an incomplete SAP_ALL Profile.

→ The following cases, are typical drivers for the regeneration of SAP_ALL profile:

* New creation of a customer-specific authorization object.
* After upgrading the system to a new release.
* After every support Package import, provided the support package contains new authorization objects.

Securing Tables:-

Introduction to Table Security:-

All data that exists in an SAP system is stored in its database.

→ Therefore, it's highly important to protect sensitive business data with proper table authorizations.

→ There are several ways to access data from a table. Users can also access the tables directly with tools like Transactions SE16, SE16N, SE17, SM30, SM31 and so on.

→ By default, those tools check for authorization objects S_TABU_DIS, and, if not successful, for S_TABU_NAM. If the table is client client-independant and a user wants to modify it, it also checks for S_TABU_CLI.

→ The authorization checks work in the following order:-

→ S_TABU_DIS is checked (always).

→ If failed, S_TABU_NAM is checked (and only if *_DIS failed!)

→ If either was sucessful and the user wants to modify a client independant table, then S_TABU_CLI is checked.

→ If S_TABU_CLI check is unsuccessful, the user will still be able to display the table since 'dis' or 'Nam' passed.

S_TABU_DIS:- It checks authorization with an activity (field ACTVT) in combination with a table authorization group (field DICBERCLS)

→ The table authorization group is a container of several tables that are similiar.

→ The authorization groups are maintained in Transaction SE54, or alternatively directly in transaction for SM30 for view V_DDAT_54.

→ When authorization S_TABU_DIS, access is granted to all tables that are assigned to a specific table authorization group.

→ SAP uses a generic group called &NC& which stands for "not classified". In an ERP system (SAP NW 7.5 EHP 8) only about 20% of the tables are assigned to an actual table authorization group; the rest belongs to "&NC&".

→ Therefore, assigning &NC& gives broad access to multiple tables and it must be very used very carefully.

→ Table TDDAT contains all table authorization group assignments for tables. This information is very helpful to identify the group of

tables that belongs to a table authorization group.

S_tabu_Nam: S_Tabu_Nam is only checked if a previous check on S_Tabu_Dis failed.

→ If S_Tabu_Dis was successful, there's no further check for S_Tabu_Nam.

↳ Therefore, S_TABU_NAM doesn't replace S_TABU_DIS but allows you to more specifically grant access to tables.

→ S_Tabu_Nam checks for an activity field (field ACTVT) and a table name (field TABLE).

S_table_Cli: If a table is client-independant and you want to maintain it, the SAP system checks for an additional objects called S_TABU_CLI.

→ When a table is client_independant, its changes can have side-effects for other clients and hence required further protection.

→ S_TABU_CLI is a complimentary authorization check after S_TABU_DIS or S_TABU_NAM as was successful.

→ S_TABU_CLI is only checked when a user wants to modify data; display access is granted without checking S_TABU_CLI. S_TABU_CLI only knows one field, CLIIDMAINT.

→ Note: To identify a table client_independant you can check if the field MANDIT (client) exists. If a table contains MANDIT, it's a client-dependant table and hence doesn't check for S_Tabu_CLI.

S_Tabu_lin: is used to protect the content of a table with line-oriented authorizations.

→ The system checks S_TABU_LIN in addition to the table authorizations mentioned earlier, like S_TABU_DIS and S_TABU_NAM. Before S_TABU_LIN is checked, all the preceding checks must be successful.

Note:- S_Tabu_lin only works after some configuration. The first step is to create an organizational criterion that's used within the authorization objects. (41)

Srikanth sir class *** Ticket issues easy steps to follow.

Please provide us the following details?

1. Kindly describe the problem in detail (step by step process).
2. Can you please let me know what are the different transactions are you trying to access?
3. What is the error message that you are getting? Please send us a screen shot of it?
4. Please provide one of your colleagues i'd who is able to execute this process successfully.
5. Please send us SU53 dump for further analysis.
6. Were you able to perform this task earlier or is this the first time that you are trying to do it.

How to make an ERRORLOG, SU53:-

Repeat the action where you have received the error message,

→ When the access fails and you receive an error message saying you have not enough authorization, please go to the command field and write the following command:

/OSU53

→ You then receive an error log on the screen.

1. Please expand all the drop downs so that all fields and values are visible to us
2. Take a screen shot of this error log with expanded drop-downs.
3. Send us the screen ~~shot~~ shot for further analysis.

Looking forward to your reply with all details mentioned.

Introduction to SU22: SAP delivers a set of authorization defaults in tables USOBT and USOBX. To access the data of those tables, you can use Transaction SU22, which contains the default values that were delivered by SAP.

→ As a customer, you can modify and extend those authorization proposals. Your custom authorization defaults are stored in tables USOBX_C and USOBT_C.

→ To check and maintain custom authorization proposals, Transaction SU24 is used.

→ With Transaction SU25, SAP provides a tool that allows security administrators to compare delivered Transaction SU22 data with Transaction SU24, and to update and modify custom authorization proposals in Transaction SU24.

→ **Note:** Never change Transaction SU22 data manually · because it's overwritten with each upgrade · Instead, use Transaction SU24 to define custom authorization proposals and use Transaction SU22 as a reference to compare custom data with SAP data.

Introduction to SU24: With SU24, a security administrator can maintain proposals for transactions, reports, functions modules, and so on.

→ In this transaction, you can maintain default values or for authority checks that are proposed in the PFCG when a transaction is added to the role. That simplifies the maintenance of a transaction drastically, as it proposes standard values that must be maintained in any case to successfully execute a transaction.

→ In addition, Transaction SU24 allows you not to maintain authorization proposals but also to deactivate certain authorization checks for certain transactions by switching the check indicator to Do Not Check.

→ In the sixth column (Proposal), we can see which objects are mandatory and hence must be maintained to successfully use the transaction. Those proposals come with the Proposal status as Yes.

→ In the fourth column (TSTCA), the proposal for the mandatory object maintained in Transaction SE93, which is checked at transaction start are displayed.

→ We can also maintain the default values for the authorization objects. However, if you want to deactivate an AUTHORITY-CHECK from the code, you can do that with the check Indicator column by changing to Do Not check.

Note:- It's only possible to change the check Indicator "Do Not Check" for ~~for~~ can analyse objects other than those for HR and BASIS.

Quick Tip:- If the data of the SU24 seems to be inconsistent in your system, you can analyse the data and repair it using the report SU24_AUTO_REPAIR.

CHECK INDICATORS:-

1) ~~Do not check~~ Yes:- These objects are ~~not~~ checked during transaction execution and also pulled into a role when the transaction is added to a role. These authorizations appear with status standard or maintained in role maintainence.

2) Do not check:- These objects are not checked during transaction execution. Authorization objects belong to Basis and HR components can not be marked as Do not checked.

3) Check, No:- These objects are checked during transaction execution but are not pulled into the role even if the transaction is added to the menu.

Expert Mode Options:-

The three available maintence types works as follows:

1) Delete and recreate profile and authorization is used to delete all the authorizations from the role and pull new data from transaction SU24. Remember, this will delete all data that has ~~per~~ previously been maintained.

2) Edit old status: is the same as the non-recommended change Authorization Data option, which doesn't consider Transaction SU24 when

you make changes to the role.

3) Read old status and Merge with new data:- is the recommended way to create and update your authorizations. In this mode, the profile generator pulls the authorization proposals from Transaction SU24 and merge them into the role.

What is the Difference between : User Group in Logon Data and Groups Tab?

→ User Group in Logon Data tab will undergo through authorization check of the authorization object S_USER_GRP where as user group maintained in Groups tab will not undergo authorization check.

→ So, the Authorization check for the user Groups maintained in GROUPS tab is to segregate the work for Administrator based on countries or locations or Depen Department whereas User Group in GRoup tab is General Segregation that can be used to perform mass maintainence.

Difference Between : Adding T-code in Menu and S_Tcode :-

→ When the T-code is added into role menu and precede to authorization tab the profile generator automatically pulls all the maintained authorization objects contains authorizations which are eventually needed for users to whom the role is assigned whereas.

→ When the T-code is added into S_Tcode manually, no authorization objects which are necessary to make T-code function properly are pulled from the tables USOBX_C and USOBT_C (SU24). If this role is assigned to the user, it will only allow user to execute the code and any further authorization check related to the t-code will fail.

→ T-code should never be added manually to S_Tcode instead it should always be added as a menu item with in a role. If not followed, it would result in several ambiguity within SAP system and your security approach will not be effective.

Difference between : Maintaining ORG level in the Top and field!-

→ When a value is maintained in org level in the top, the same value reflects in all the fields available in the role whereas when the value is maintained in a field, it reflects in the authorization object.

→ To convert a field to org. level, the report PFCG_ORGFIELD_CREATE is used whereas to bring a org level back to a normal field the report PFCG_ORGFIELD_DELETE is used.

→ The fields 'ACTVT' and 'TCD' can't be be converted to org. levels.

* With SAP Net Weaver 7.50 Support Package 9, SAP provides new functionality to promote authorization fields to customer specific organizational levels. You can get more information from SAP note 2271536. (FAQ / use of customer-specific organizational level in PFCG).

Note:- former Reports like PFCG ORGFIELD CREATE PFCG ORGFIELD DELETE, PFCG ORGFIELD UPGRADE are obsolete and you are required to use transaction SUPO.

Transport System in SAP:- Technically, the SAP system supports your organizational change process with the transport system.

→ Changes that you make to the system are automatically recorded and bundled in transport requests.

→ When a transport request has been released, you can transport the changes to downstream system within multisystem landscapes usually consisting at least of a development, testing, and production system.

Note: Advantage with transport is, you don't have to implement the change manually in each system.

Transport objects in SAP:- The target and purpose of a transports is to transfer objects and configurations from one system to another.

→ In the common three-system landscape, a transport is generated in the development system, transported to the QA system where it is tested, and finally imported to the production system.

Types of Objects in SAP:-

1. Client dependent and
2. client independent.

Data which can be accessed across all the clients are client independent.
Data which can be accessed in a specific client are client independant (use MANDT field in table).

Note: A client-~~in~~dependant table has the field MANDT of data type CLNT, which indicates client id.

→ A client independant table does not have this field.

Types of Transport Requests:- The request type depends on the object that is supposed to be transported. There are two types of Transport Requests.

1. Customizing Requests:- Are used for customizing changes, such as the maintainence of tables.

→ Customizing Requests are client dependant Requests.

2. Workbench Requests:- Workbench requests are used for repository changes (programs for example).

→ Workbench Requests are client Independant Requests.

Note:

→ The changes to the customizing cannot be transported with a workbench request and vice versa.

→ That means, when creating the transport request, you need to know if you want to change a customizing or repository object. You cannot change the transport request type retroactively.

Creating Transport Request:- To transport an object, you have to create a transport requests in which you enter you change. You can create the transport request before implementing the change or during the recording in a respective dialog.

→ Transpost requests can be created using the following T-codes: SE01, SE09 and SE10.

Transport files:-

→ A transport request consists of a control file (co file) and a data file. (→ user details, time, when work and all)

→ The control files start with 'K' and are stored in the <drive>:\usr\sap\trans\cofiles (Windows) directory.

→ The data files start with 'R' and are stored in the <drive>:\usr\sap\trans\data (Windows) directory.

Possible Return Codes:- The following return codes are possible:

* 0 : Successfully Completed.
  4 : Ended with Warning.
  8 : Ended with Errors.
  12 or higher : Transport has not been executed.

E070 : change & Transport System : Headers of Requests/Tasks
E071 : change & Transport System : object Entries of Requests/Tasks } Tables related to Transport-ing.
E07TT : change & Transport System : Short Texts for Requests/Tasks

---

Important Terminologies to be used:-

1. Execute the Report
2. Brows the table (or) Display the table.
3. Maintain values in the field.
4. Maintain check proposals
5. Generated a Profile.
6. Assign the Role to the user.
7. Perform User Comparision
8. Schedule a Background Job.
9. Add T-code into the menu
10. Search for the Role
11. Released the transport Request
12. Maintain table in the Authorization Group.
13. Moved Transport Request from Dev to QAS (or) from QAS to PRD.

Daily / weekly / Monthly checks in Activities in Real time:-

→ Monitoring the standard background jobs whether they are successfully executed (or) not (SM37).

→ Monitoring the list of users who are currently logged in into SAP (SM04 (or) $'ALOS).

→ Monitoring the list of users having access to SAP_ALL (weekly as it is critical).
(SUIM → Users → Users by Complex Selection Criteria).

→ Monitoring the list of users having access to SAP_NEW
(SUIM → Users → Users by complex selection criteria).

→ Monitoring the list of user groups.
SE16N → USGRP.

→ Monitoring the list of users who belong to the group SUPER
SE16N → USGRP_USER

→ Monitoring the list of Dialog Users
(SA38 → RSUSR200) / SUIM → users → UBLSC → execute → filter at user (Dialog).

→ Monitoring the list of system users.
SA38 → RSUSR200

→ Monitoring the list of users who are not valid today
SA38 → RSUSR200

→ Monitoring the list of users who are locked by Administrator.
SA38 → RSUSR006.

→ Monitoring the list of users with Incomplete Address.
SA38 → RSUSR007.

→ Monitoring the list of users who have not logged in the last 90 days.
SA38 → RSUSR200.

→ Monitoring the list of Roles that are created in this month.
SUIM → change Documents → for Roles.

→ Monitoring the list of users that are created in this month.
(SUIM → change documents → for users)

→ Monitoring the list of users that are locked or deleted in this month.
SUIM → change documents → for users.

→ Monitoring the list of user having access to SE16, SE16n, SA38, etc.
SUIM → Users → users by complex selection criteria

→ Monitoring the list of Z tables that are part of the Authorization group &NCF.
SE16n → TDDAT → Table name = Z* and Auth. Group = &NCF.

→ Monitoring of the passwords of the standard users are changed or not.
SA38 → RSUSR003.

→ Monitoring the list of illegal passwords in the systems.
SE16n → USR40

→ Monitoring the login parameters in the system.
(SA38 → RSUSR003) (or) RSPFPAR_LOGIN.

→ Monitoring of the standard user SAP* is protected against misuse.
Parameter: login/no_automatic_user_sapstar should be >0.

→ Monitoring the list of developers in the system.
(SE16N → DevAccess)

→ Monitoring the list of users having access to S_Develop with activity 01 (or) 02 in Production system.
(SUIM → Users → users by complex selection criteria).

→ Monitoring the list of users having access to S_TABU_DIS with access to authorization Group &NCF
SUIM → users → Users by complex selection criteria.

→ Monitoring the list of users having access to S_RFC_ADM.
SUIM → Users → User by complex Selection Criteria.

→ Monitoring the list of RFC's that are created
SE16n → RFCDES.

→ Monitoring the list of logical systems that are created. (SD)

SE16N → TBDLS

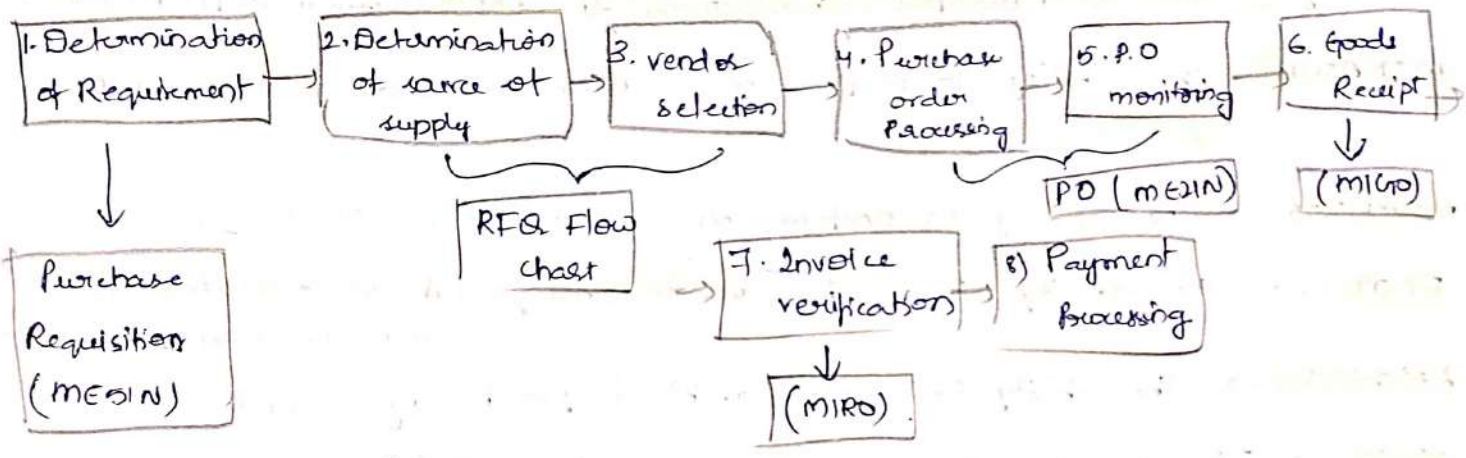
→ Monitoring the list of clients in the system.

SE16N → T000.

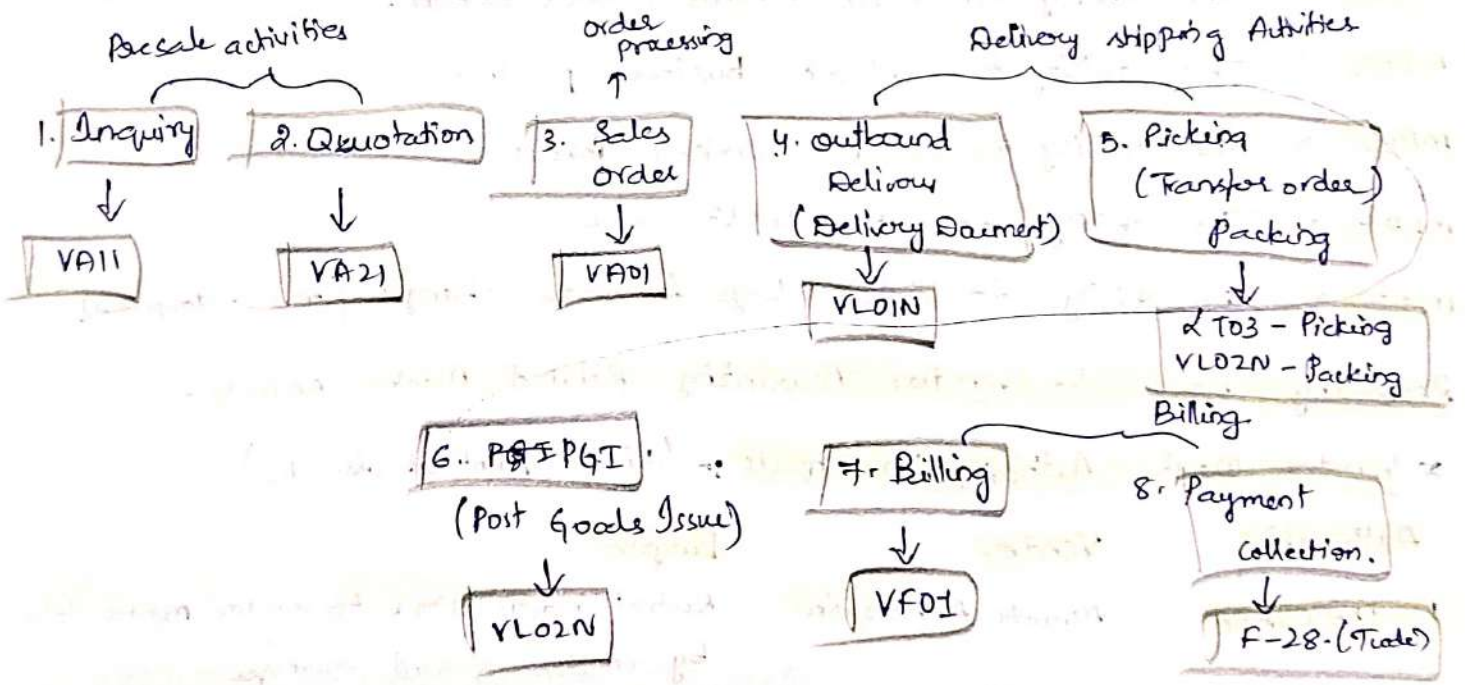
→ Monitoring the list of Org. levels in the system.

SE16N → USVAR.

Procurement Cycle:-



Order to Cash Business Process (Related to SD-Sales Department).



Billing

Preventing SOD conflicts (Seperation of duties) Conflicts in P2P cycle:-

It must have this access
Create / maintain PO's

Approve PO's

he should not have this access
Maintain vendor master data

Receive goods against Those PO's

Maintain vendor Master data.	Reversile reconcilation accounts.
Maintain vendor master data	Create/Maintain Vendor Payments.
Process Goods receipts	Create/ maintain vendor payments.
Process Goods receipts	Create/maintain PO's
Process Goods receipts	Maintain Vendor master data.
Process Goods receipts	Maintain material master data.

Limiting Access To Powerful Transactions in P2P:- (T-codes in MM and P2P point of view).

MEMASSIN – The ability to perform mass maintainence on purchase info records.

MEMASSPO – The ability to perform mass maintainence on PO.

FK09 → The ability to confirm vendor changes (if user have this he will also have XK09).

RM06ID47 → The ability to delete archived purchasing records.

XK99 → The ability to perform mass vendor maintainence

MK06 → The ability to delete vendor master data.

MK05 → The ability to unblock business partners.

MR02 → The ability to process blocked invoices.

MRHG → The ability to enter credit notes

MSL2 → The ability to delete logs for mass changes (MSL. (dangerous).

Restricting changes to vendor Accounting Related Master Records:-

* **Vendor Master Authorization objects** :- (finance point of view 'F_')

Auth. obj	Vendor	Purpose
F_LFA1_BEK	Accounts Authorization	Restrict modifications to vendor master data by vendor account group.
F_LFA1_BUK	Authorization for company codes	Restrict the ability to change the vendor by company code.
F_LFA1_GRP	Authorization by Account group	Restrict the ability to change the vendor based upon account group.

F_LFA1_AEN	Change Authorization for Certain fields	Restrict modifications to vendor master data by defined fields.

(51)

Vendor Account Group:-

→ A vendor account group is a classifying feature of vendor master records in SAP ERP. It determines the following.

1. Interval from which a unique number is assigned to a vendor.
2. Whether the number is assigned by the user (external number assignment) or by the system (internal number assignment).

→ A vendor account group can be accessed using the T-code OBD3 and the table where vendor Account Group is stored is T077K. (table).

Restricting changes to Material Master Records:-

Material Management Auth. objects:-

Auth object	Material Master	Purpose
M_MATE_BUK	Company codes	Restrict modifications to material master data by company code
M_MATE_WRK	Plants	Restrict modifications to material master data by plants.
M_MATE_MAR	Material Types	Restrict the ability to change the material master data by material type.

Restricting changes to Goods Receipts:- SAP provides a variety of mechanisms to restrict changes to goods changes to goods receipts changes to goods receipts, including plant and movement type. Key authorization objects for this are.

Auth. obj	Goods Receipt for PO	Purpose
M_MSEG_BWE	Movement type	Restrict modifications to goods receipt by movement type. (plays a major role in MM).
M_MSEG_WWE	Plant	Restrict modifications to goods receipt by plant.

Note: No one should have * access in movement types.

Movement Types:-

→ When you enter goods movement in the MIGO transaction or any other transaction dealing with material documents, you need to specify

SAP Movement Types.

→ SAP movement Type is a three-character key which differentiates various material movements, E.g. Goods Receipt, Goods Issue or Transfer Posting.

Restricting change to Banking Master Records:- (Critical Auth. objects)

→ The ability to change banking data should also be tightly restricted, as bank account information can be highly susceptible to fraud.

→ SAP provides a variety of mechanisms to restrict changes to banking master records.

Auth. object	Banks	Purpose
F_BNKA_BUK	Authorization for company codes	Restrict modifications to house banks and bank accounts company code.
F_BNKA_MAN	General Maintenance Authorization	Restrict the general ability to maintain bank master data.

Preventing SOD conflicts in O→C cycle:-

If user have this access	He should not have access to this.
Process Sales Orders	Maintain Pricing Conditions.
Process Sales orders	Issue free of charge delivers.
Process sales order	Post customer payments.
Process Sales order	Released blaked documents
Create Billing Documents	Maintain customer Master Data.
Create Billing Documents	Post customer payments
Create customer credit memos.	Release Blocked documents.

Create customer credit memos — Maintain Pricing conditions.

Create customer Credit memos — Post customer Payments.

Limiting access to powerful T-codes in O2C:-

XD99 → The ability to perform mass maintainence.

VD06 → The ability to delete customer master data.

program RFDKLI50 → The ability to perform mass changes on customer credit limits.

VD05 → The ability to unblock business partners.

VKM1 → The ability to unblock sales orders with a credit block.

FB75 → The ability to enter customer credit memos.

Restricting changes to Customer Master Records:-

→ Customer masks data is generally managed centrally, with specific permissions related to sales and accounting details. Customer data can also be managed directly within SD and SAP ERP Financials Financial Accounting.

→ SAP provides a variety of mechanisms to restrict changes to customer masks records, including account, application, company code, account group, or specific fields within the customer master.

Customer Master Authorization objects:-

Auth. object	Customer Master	Purpose
F_KNA1_BED	Customer: Accounts Authorization	Restrict modifications to customer master data by customer account range.
F_KNA1_BUK	Customer: Authorization for company codes	Restrict the ability to change the customer by company code
F_KNA1_KGD	Customer: change Authorization for Accounts Groups	Restrict the ability to change by customer account group.
F_KNA1_AEN	Customer: change Authorizations of for certain fields.	Restrict modifications to customer master data by defined fields.

Account Groups:- Account group is the highest level of customer master data. Customers are classified into various Account Groups.

→ Account Group functionalities are:

* Controls the field of Customer Master
* Classifies Customers to use for various functions.
* Lists the Partner functions.

→ The T-code OBD1 is is used for Creating Account Group.

* Examples of Account Groups are: Franchise, Wholesale Customer, Competitor, Prospective Customer Etc.

Restricting changes to View/Maintain Payment Card Data:-

Payment Card data Authorization objects:-

Auth. objects	Payment Cards	Purpose
B_CARD_SEC	Payment Cards: Authorization Encryption Card master	Restrict the ability to encrypt or decrypt payment card data.
B_CCARD	payment cards: payment cards.	Restrict the ability to maintain (or even view) payment card data.

→ Data privacy issues have taken the headlines in the last few years.

→ When dealing with payment card information such as credit cards, risks extend beyond the ability to maintain the information and migrate into the ability to view the data as well.

→ SAP provides a variety of mechanisms to restrict access to payment card master records.

Restricting Ability to Maintain Pricing Conditions:-

→ The integrity of pricing conditions is critical to sales processing.

→ SAP provides a variety of mechanisms to restrict access to pricing condition master records.

→ Security permissions can restrict pricing condition maintenance by sales organization or by condition type.

Pricing Conditions Authorization objects:-

Auth. object	Payment Cards	Purpose:
V_KONH_VKO	Condition: Authorization for sales organization	Restrict the ability to maintain conditions by sales organization distribution channel, and division.
V_KONH_VKS	Condition: Authorization for Condition Types.	Restrict the ability to maintain conditions by condition type.
V_KONG_VWE	Generation of conditions: Authorization for Usage/ Application.	Restrict the ability to generate condition tables.

Transport Related Questions:-

Q) Which Table stores the details of an Unreleased change Request?

A) Table E070CREATE - Creation Information.

→ It consists creation information of non released Transport Requests once They are released, entry from E070CREATE is removed.

Q) How do you check who has released a Transport request and who has imported a Transport request into production?

A) Use the table TPALOG to check this:

On Dev System: TRSTEP = E (→ export) ⇒ ADMIN has released the transport.

On Prod System: TRSTEP = I (→ import) ⇒ ADMIN has imported the transport (or) (01)

You can see this also in

T-code SE01/SE10 with Go to → Action Log

T-code STMS → Import History → Edit → Display More.

3) How do you get the list of Transport Requests released or modified for a particular date? (SAP)

A) 1. From T-code SE01, using a date range (from transport tab).
2. Using table E070 and E071. You can find the date range.
3. Using T-code STMS. Go to Extra → Settings. (BASIS T-code)

↳ SE01 → Transport → ☑ Released [ ] → set date → Display.

4) How will you get the list of Transports that are moved to QAS and not to PRD?

A) . STMS → System → Import → from QAS. & same login to PRD same method.

→ There is no direct way using STMS to get this info. You can download the import history of QAS and PRD separately and do a vlookup using excel.

5) Which Table stores the Information about Transport Request?

A) Tables E070 & E071.

6) How do you delete trace files from STO1?

A) we cannot delete it from T-code STO1, we have to delete them (Trace files) manually

→ There is no option to delete this file from STO1. You must delete this file manually from OS.

7) How can I resolve this error from in STO1?

"ERROR when writing the Trace. No such file or directory". (common issues in Trace) this will be done by BASIS Team we need to inform them.

A) Ensure the directory /usr/sap/$SID/DVEBMGS00/log exists and the file will be created by default name Trace.

SU53 Introduction:-

Troubleshooting security issues is one of the daily tasks of any security administrator. The first method of investigating authorization failures is by using SU53 transaction.

→ The SU53 window shows the last check for an authorization which has returned a non zero value (authorization failure) for the user.

De-Activating SU53 T-Code:-

To deactivate this function, set the system profile parameter auth/check_value_write_on to '0' (zero).

What happens behind the scenes in SU53?

→ When a user runs transaction SU53, the system loads data into tables USR07. The table is populated with a single record containing information relevant to this denial.

STO1:- Introduction:-

→ In normal days cases, when a user receives an authorization error, the end user will execute Transaction SU53; This transaction shows that the last authorization check failed.

→ However, you'll find that this error log isn't sufficient to resolve the problem all the times.

→ In these cases, you'll find it necessary to perform an authorization trace during a user session with Transaction STO1.

Steps to perform using STO1:-

To place a trace on a user, execute Transaction STO1 and flag the authorization check indicator under the Trace components box.

→ After setting Transaction STO1 filters, click on the Trace on button.

→ From this moment until you click on Trace off, all activities performed by the user are logged depending on your earlier settings. After the user completes the test session and after you terminate the trace, you can analyse the activities performed by the trace by clicking on the Ana Analysis button.

Return Codes in

Important Points when using STO1:-

Transaction STO1 is application server dependant. If your system has more than 1 appl°. server, you have to be sure that the trace is performed in the same application server the user is logged into.

→ Take a look at time zone and clock. If the application server has a time that is different from your PC, then during your analysis after performing the trace, you might select a trace log outside the time recorded.

→ You can view in what application server a user is currently logged in to by using Transaction AL08 (or) SM04 by asking the user directly - he can see the application server name in the bottom-right area of SAP GUI.

Return codes in STO1:-

RC = 0 → check for Authorization Successful.

RC = 4 → check for user is having the Auth. object with a different value

RC = 12 → User doesn't have the required Auth. object.

Background Jobs:-

Necessity for comparing User Master Records:

To ensure that only authorization Profiles which are valid are contained in the user master record each day, you must execute a daily profile comparision.

→ There are two ways to execute user master comparision. They are:

1. Using the transaction PFUD, for user master compare.
2. As a background job before the start of each day by executing the report PFCG_TIME_DEPENDENCY.

PFUD - SAP User Master Data Reconciliation:-

→ The transaction code PFUD performs the user master comparision for the multiple roles at a time.

→ User master comparision for individual roles can be performed from transaction PFCG.

→ It can be executed in dialog, or to schedule it as a complete comparision in the background.

PFCG_TIME_DEPENDENCY:-

* PFCG_TIME_DEPENDENCY (technical name of the program RHAUTUPD_NEW) is used to keep the authorization data of user master in current status.
* It checks the validity of "Profile" in the user master and removes them if there are any expired profiles.
* Thus you don't need to check every user daily about the expired roles to remove their profile.
* Ideally, PFCG_TIME_DEPENDENCY must be executed midnight (OR) once in 24 hours.

PG PRGN_COMPRESS_TIMES:- The Report PRGN_COMPRESS_TIMES is used to delete expired roles from user master records and remove duplicate role assignments.

→ It can be scheduled on a weekly basis.